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

Susan Symington
The MITRE Corporation
McLean, VA

William Polk
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

September 8, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.09082020-draft

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

Abstract

Internet of Things (IoT) devices are typically connected to a network. The steps performed to provision a device with its network credentials are referred to as *network-layer onboarding* (or simply, *onboarding*). This paper proposes a taxonomy for IoT device onboarding that can clearly express the capabilities of any particular onboarding solution. By providing a common language that describes and clarifies various onboarding characteristics, this taxonomy assists with discussion, characterization, and development of trusted onboarding solutions that can be adopted broadly. To provide context for the proposed onboarding taxonomy and to try to ensure its comprehensiveness, this paper also describes a generic trusted onboarding process, defines onboarding functional roles, discusses onboarding-related aspects of IoT lifecycle management, presents onboarding use cases, and proposes recommended security capabilities for onboarding.

Keywords

application-layer onboarding; authentication; bootstrapping; credentials; device lifecycle management; identity; internet of things (IoT); network-layer onboarding; onboarding

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's cybersecurity programs, projects, and publications, visit the National Cybersecurity Center of Excellence (NCCoE) and the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

Public comment period: *September 8, 2020 through October 8, 2020*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: mitigating-iot-ddos-nccoe@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Acknowledgments

The authors wish to thank the following individuals for the generous contribution of expertise and time that they demonstrated by attending a Cisco-hosted meeting and expressing their views on many of the onboarding-related topics covered in this paper. We have developed the content of this paper, in large part, based on the discussion that ensued at that onboarding meeting.

Name	Organization
Allaukik Abhishek	Arm
Anurag Gupta	Arm
Reed Hinkel	Arm
Darshak Thakore	CableLabs
Mark Walker	CableLabs
Owen Friel	Cisco
Russ Gyurek	Cisco
Eliot Lear	Cisco
Peter Romness	Cisco
Bob Sayle	Cisco
William Barker	Dakota Consulting
Katherine Gronberg	Forescout
Nils Gerhardt	Global Platform
Saurabh Dadu	Intel

Name	Organization
Drew Cohen	MasterPeace Solutions
Geoff Matrangola	MasterPeace Solutions
Kevin Yeich	MasterPeace Solutions
Janet Jones	Microsoft
Parisa Grayeli	The MITRE Corporation
Josh Klosterman	The MITRE Corporation
Blaine Mulugeta	The MITRE Corporation
Doug Montgomery	National Institute of Standards and Technology
Ranga Mudumbai	National Institute of Standards and Technology
Monika Singh	National Institute of Standards and Technology
Matt Tooley	NCTA – The Internet and Television Association
Michael Montemurro	Wi-Fi Alliance/Blackberry
Steve Clark	WISeKey

Audience

The audience of this paper is intended to include IoT device manufacturers, integrators, and vendors; managers of networks to which IoT devices connect; service providers (internet service providers/cable operators and application platform providers) who want to simplify the IoT device connection process for their customers; industry consortia; standards development organizations; and any other individuals or organizations that are stakeholders in the effort to define open, standard, trusted, and scalable solutions for efficiently and easily providing IoT devices with the network credentials that they need to become operational.

Table of Contents

List of Figures

List of Tables

List of Appendices

1 Introduction

Internet of Things (IoT) devices are typically single-purpose, smart objects that are connected to each other, to other components on a local network, or to a cloud via a network to provide functional capabilities. As with any device, to connect to a network securely, an IoT device needs appropriate credentials. A typical commercially available, mass-produced IoT device cannot be pre-provisioned with local network credentials by the manufacturer at manufacturing time. Instead, these local network credentials have to be provisioned to the device at deployment. We refer to the steps that are performed to provision a device with its local network credentials as *network-layer onboarding* (or simply *onboarding*).

The wide variety of IoT devices differ regarding power, memory, computation, and other resource characteristics. Another key difference among these devices is in how they are onboarded. Ideally, the onboarding process should be trusted, efficient, and flexible enough to meet the needs of various use cases. Because IoT devices typically lack screens and keyboards, trying to provision their credentials can be cumbersome. For consumers, trusted onboarding should be easy; for enterprises, it should enable large numbers of devices to be quickly provisioned with unique credentials. Security attributes of the onboarding process assure that the network is not put at risk as new IoT devices are added to it.

This paper proposes a taxonomy for IoT device onboarding that can be used to clearly express the capabilities of any particular onboarding solution. By providing a common language that describes and clarifies various onboarding characteristics, this taxonomy assists with discussion, characterization, and development of onboarding solutions that can be adopted broadly. To provide context for the proposed onboarding taxonomy and to try to ensure its comprehensiveness, this paper also describes a generic onboarding process, defines onboarding functional roles, discusses onboarding-related aspects of IoT lifecycle management, presents onboarding use cases, and proposes recommended security capabilities for onboarding.

1.1 Challenges with current onboarding mechanisms

Some of the mechanisms that are currently used to perform IoT device onboarding are fragmented or insecure. For example, typical devices that are onboarded to most consumer home wireless Wi-Fi networks currently all use the same pre-shared key to connect to that network. If multiple networks are available, an IoT device selects the network to connect with and provides the network password (i.e., the pre-shared key). Without a screen or keyboard, the processes of selecting the correct network to which to connect and providing the device with the network password can be difficult. To make these steps easier, some devices have been equipped with Wi-Fi Protected Setup (WPS), an onboarding mechanism that enables a consumer to onboard IoT devices by simply pressing a button that causes the network router to provide the devices with the password that they need to connect to the network. While this onboarding mechanism does an excellent job of making device onboarding easy and efficient for the consumer, it has unfortunately been shown to suffer from several security vulnerabilities [1]. In addition, it also requires a physical button, which can be cumbersome if the device is not physically accessible.

Given the threats faced in today's internet, there is a desire for more security than can currently be provided by the same shared password for all devices on a network. Under a shared-password model, if a device presents the correct password, it will be permitted to connect to the network. The network's decision regarding whether to grant a device access to the network has nothing to do with the individual identity of the device or the device's type. Furthermore, although networks can falsely identify themselves, the device is not typically provided with any way to verify that the network to which it is connecting is the intended network. To address these problems, the typical consumer network onboarding process needs to be improved [2].

In contrast to the home environment, onboarding in an enterprise environment is typically based on a more robust security model that requires each device to have its own distinct credential to connect to the network. However, this often means that the onboarding process is complex and resource intensive. Currently, the onboarding process typically takes more than 20 minutes per device and requires coordination and sometimes entails conflict and tension among installation technicians, information technology (IT) network/security operations, and operational technology teams [3]. When onboarding is performed manually, it is time consuming. If it requires individuals to have access to device credentials, it is vulnerable to the risk of those credentials being disclosed to unauthorized parties. Some enterprises require the ability to perform bulk onboarding—i.e., to provide many IoT devices with their network credentials quickly—which necessitates that the onboarding process be automated and zero-touch. However, most zero-touch solutions on the market today require that the onboarding credentials of the network to which the IoT device will connect be built into the device at the point of manufacture [3]. This effectively requires a manufacturer to uniquely configure individual devices to enable onboarding for each customer and use case, on a build-to-order basis, which is inefficient and expensive. It requires the device manufacturers to collect each customer's unique requirements, a process that can take weeks to complete and requires the engagement of multiple parties [4]. Then, the manufacturer configures the devices to specific customer needs (e.g., credentials/keys specific to the device's target network are loaded by the manufacturer), which, once completed, requires multiple rounds of testing with various parties within the customer organization that may take as long as three weeks to complete [4]. Next, training is required, involving preparation of unique instructions. When the customer receives the device, activation of the device on its target network often requires the customer to complete a long list of manual steps. The complexity of the process, combined with the fact that it is susceptible to human error, make it vulnerable to security risks.

Customizing each device's onboarding credentials at the point of manufacture in this manner is clearly inefficient, complex, and potentially insecure. To take full advantage of economies of scale, a manufacturer should be able to build identical devices for all its customers. Making such a uniform manufacturing process possible requires an onboarding solution that can securely provision each device with unique onboarding credentials at the time of deployment on the local network (rather than at the time of manufacture). Ensuring that such an onboarding solution is trusted requires the credentials to be provisioned to the device over an encrypted channel by using a process that does not provide anyone with access to the credentials, thereby protecting the credentials from disclosure to unauthorized parties. Defining the characteristics of such a trusted onboarding solution is the objective of this paper.

1.2 Genesis of This Paper

A case can be made for standardization of one or a small number of onboarding solutions that are trusted, efficient, scalable, and flexible enough to meet the needs of various use cases. Ideally, these solutions can be developed with broad community input, solving the onboarding problem for the benefit of all, with open, readily available standards. With that objective in mind, this paper was developed based on discussions with representatives from a wide variety of IoT stakeholder communities: device manufacturers, integrators, and vendors; enterprise network administrators; industry consortia; and members of standards development organizations. Requirements, objectives, and use cases representing varying viewpoints were discussed to help capture a broad community perspective regarding onboarding challenges and solutions.

This paper proposes a taxonomy for IoT device onboarding that can be used to clearly express the capabilities of any particular onboarding solution. By providing a common language that describes and clarifies various onboarding characteristics, this taxonomy helps develop onboarding solutions that can be adopted broadly.

1.3 Objectives

The objectives of this paper are to:

- propose a taxonomy for IoT device onboarding that clearly expresses the capabilities of any particular onboarding solution
- promote this taxonomy as a common vocabulary to be referenced in future work as a means for describing and classifying characteristics, roles, use cases, steps, challenges, and other information related to IoT device onboarding
- elicit feedback from IoT device manufacturers, IoT device users, service providers, industry consortia, standards development organizations, and other stakeholders to ensure that the taxonomy fully captures the elements required to define and compare onboarding solutions in product-agnostic terms
- encourage stakeholders to use the taxonomy to express their onboarding requirements, clarify what characteristics are required, and specify the optional capabilities to clearly bound the onboarding challenge
- propose recommended security capabilities for onboarding and solicit feedback for the recommendations

1.4 Scope

This document does not consider network access methods that do not use the internet protocol (IP). It assumes that IoT devices that use non-IP access methods such as Bluetooth low energy, ZigBee, Zwave, or 802.15 radio will connect to the IP network through a gateway. Only network-layer onboarding using Wi-Fi, wired Ethernet access technologies is in scope at this time. Most of the discussion and illustrations focus on Wi-Fi use case scenarios.

1.5 Assumptions

This white paper makes the following assumptions:

- The first operation of an IoT device is to onboard itself [5]. This process should be automated and trusted.
- When initially procured, an IoT device will not have already been customized to target it to the specific local network on which it will be deployed. Manufacturers will not be required or expected to bind an IoT device to a specific network at manufacturing time; two devices of the same make and model that will be used on distinct networks will be built identically. The only difference between these devices will be their bootstrapping credentials, including their device identifier (see Section 2.5), which distinguish the devices from each other but have nothing to do with the networks on which the devices will be installed.
- IoT devices may lack screens and keyboards, making it necessary to interact with them via some sort of network communication protocol.
- Trusted onboarding solutions should:
    - be based on open standards
    - minimize the amount and difficulty of user interaction required, thereby making them resistant to human error
    - provision network credentials to the device at the time of the device's deployment on a network (rather than at its time of manufacture)
    - provide the device and the network the opportunity to authenticate each other
    - be able to provision each device with unique network credentials
    - provision the device's network credentials over an encrypted channel to protect the confidentiality of the credentials
    - not provide any individuals with access to the credentials, thereby eliminating the risk of having those credentials disclosed to unauthorized parties
    - support both wired and wireless network access
    - address various versions of both consumer and enterprise network use cases but not necessarily with the same protocol/technologies
- It is preferable to define as few onboarding solutions as possible to adequately cover all use cases because:
    - this will promote interoperability
    - there is limited real estate available on a typical chip, and the device using that chip will be required to support the onboarding mechanism that the network requires, so the fewer solutions, the better
    - this will reduce the number of code paths that need to be maintained, thus reducing manufacturing complexity and cost

2 Definitions

The term *onboarding* does not have a well-established meaning and is not used consistently in the literature. Onboarding is sometimes used as a synonym for bootstrapping and at other times is defined as a subprocess of bootstrapping [6]. In this section, we propose definitions for onboarding, bootstrapping, and other related terms. These definitions are adapted from definitions that were proposed during stakeholder onboarding discussions [7], in which bootstrapping was defined as a subprocess of onboarding.

All the terms defined in this section are illustrated in the four-step diagram depicted in Figure 2-1. The first step of Figure 2-1 depicts bootstrapping (Section 2.4) an IoT device to a network onboarding component (Section 2.3) as well as bootstrapping a network onboarding component to an IoT device. It is assumed that the device has already been provisioned with device bootstrapping credentials (Section 2.5) and that the network onboarding component has already been provisioned with network bootstrapping credentials (Section 2.6) before bootstrapping began. If the device has a device information declaration (Section 2.7), it will also already have been created before bootstrapping began, and it will be consulted as part of the bootstrapping process.

The first and second steps of Figure 2-1 together depict the network-layer onboarding (Section 2.1) of that IoT device, during which it is bootstrapped (Step 1) and then provisioned (Step 2) with its onboarding credentials (Section 2.2). The third step of Figure 2-1 depicts the device using its newly provisioned onboarding credentials to establish a secure connection with the network. The fourth step of Figure 2-1 depicts the device performing application-layer onboarding (Section 2.8), i.e., connecting to controllers, application servers, and cloud services, as directed by the device's onboarding credentials, and permitting those controllers and servers to securely install applications on the device that are needed to enable the device to fulfill its intended function and to manage the device throughout its life cycle.

Each of the terms depicted in Figure 2-1 is defined more fully in the subsections that follow the figure.

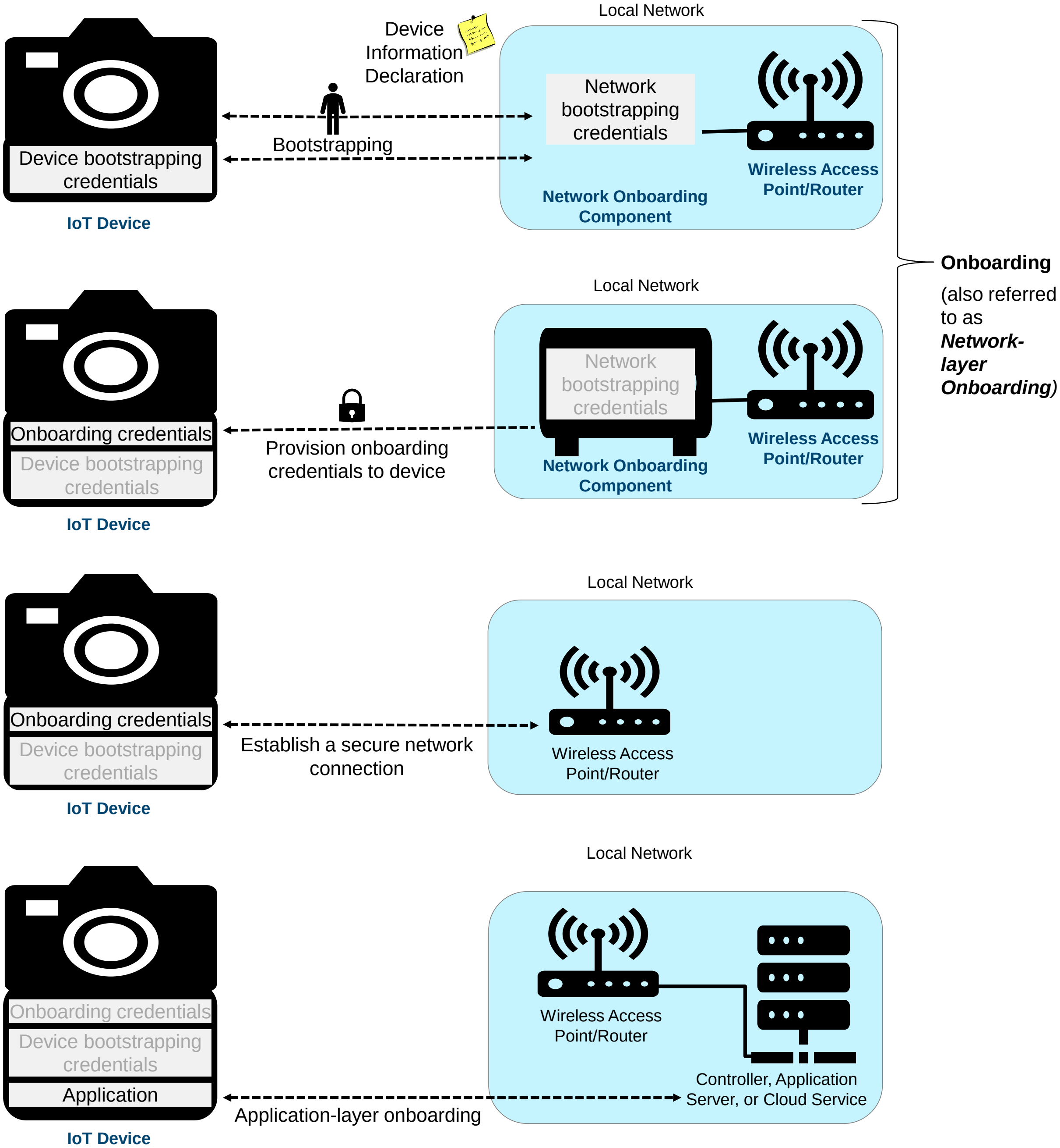

Figure 2-1 Onboarding and related terminology

2.1 Onboarding

Onboarding (as shown in the first two steps of Figure 2-1) consists of any and all steps required to provide a device with the network credentials (and possibly other information) it needs to connect securely to the network to be operational. It includes the subprocess of bootstrapping and then, after the device and the network onboarding component have established a secure channel as a result of bootstrapping, the remainder of the onboarding process consists of using this secure channel to provision the device with its onboarding credentials. Onboarding, as defined here, is also synonymous with the term network-layer onboarding.

2.2 Onboarding Credentials

Onboarding credentials (as shown in the second step of Figure 2-1) are credentials that are provisioned to the device during the onboarding process by the network onboarding component. Provisioning these credentials to the device is the goal of the onboarding process. At a minimum, they should include the credentials that the device requires to connect to the local network. They may include information such as:

- credentials needed for the device to connect to the local network (e.g., network identifier, network password, pre-shared key [PSK], X.509 certificate, and associated private key)
- additional configuration information (e.g., uniform resource locators [URLs] for reaching controllers or servers) to enable the device to become operational at the application layer once it has securely connected to the network at the network layer

2.3 Network Onboarding Component

A *network onboarding component* (as shown in the first two steps of Figure 2-1) is connected to a specific network. It represents the network to IoT devices that are not yet connected to the network, interacts with them on behalf of the network, and is authorized to determine whether they can join the network. (Note that the IoT device is permitted limited communications capabilities to perform the onboarding process. For example, a device may communicate with the onboarding component at Layer 2 or 3 during onboarding, but it will not be provisioned with a routable IP address until onboarding completes.)

As its name makes clear, the network onboarding component performs onboarding for devices that will be allowed to connect to the network securely. The network onboarding component interacts with devices by using the network onboarding protocol. It is the entity that securely provisions each IoT device with its onboarding credentials, i.e., the credentials that each device needs to establish secure network associations. Once these credentials are provisioned, the network onboarding component's work is done, and the IoT device thereafter interacts with the network directly rather than via the onboarding component unless and until the device needs to be provisioned with new onboarding credentials. Section 4 describes examples of when a device might need to be re-onboarded, which may include the device being reset to factory status, the device's certificate being renewed, or the device's key requiring rotation.

The network onboarding component may not be implemented in a single piece of equipment or as a stand-alone piece of equipment. Depending on the onboarding solution and how it is implemented, the service provided by the network onboarding component may be provided by a combination of elements. The important concept to understand is that before a device has the credentials it needs to connect securely to a particular network, some sort of intermediary is required to interact with the device on behalf of that network, to facilitate the onboarding process. The network onboarding component is the term we use to refer to this intermediary.

2.4 Bootstrapping

Bootstrapping (as shown in the first step of Figure 2-1) is a subprocess of onboarding. It provides just enough introduction and information exchange between a device and the network onboarding component to establish a secure channel over which provisioning of the device's onboarding credentials can occur. Bootstrapping consists of:

1. Initial establishment of trust/introduction between the device and the network onboarding component:
   - This introduction may be performed as an out-of-band (OOB) process.
   - This introduction may require human interaction (e.g., the device onboarder may provide the network onboarding component with information regarding the device, may provide the device with information regarding the network onboarding component, or both).
   - The trust established may be either mutual or one-way.

2. Subsequent provisioning of keys or other credentials and configuration information to the device:
   - These keys and configuration information, along with the trust that has been established in #1, result in establishing a secure channel between the device and the network onboarding component. For the utmost security, it is preferable for this protected channel to be unique, with a one-to-one binding between the device and the onboarding component, because it will be used by the onboarding component to provision the device with its onboarding credentials.

2.5 Device Bootstrapping Credentials

Device bootstrapping credentials (as shown in the first step of Figure 2-1) are credentials that a device requires to establish communications with and be authenticated by the network onboarding component. Device bootstrapping credentials may be provisioned to the device during manufacturing. They have to be provisioned to the device before it initiates the onboarding process. They pertain only to the device and not to any network to which the device may be onboarded, so, once installed, they should not change over the lifetime of the device. Device bootstrapping credentials may include information such as:

- device identifier (e.g., X.509 certificate–DevID, Device Identifier Composition Engine [DICE] Compound Device Identifier [CDI])
- secret (e.g., private key, public/private key pair, pre-shared key)
- Wi-Fi channel that the device will use
- URL of Manufacturer Usage Description (MUD) [8] file associated with device

The device bootstrapping credentials always include some sort of secret (e.g., a key or keys), which the device will use to:

- authenticate itself to the network onboarding component
- establish a secure communications channel with the network onboarding component

To protect the secret from being disclosed, it should be safeguarded in a secure storage element that prevents it from being easily extracted, modified, or tampered with without detection. Note that because the device bootstrapping credentials should not change over the lifetime of the device, if the credential is a certificate, it should not expire.

2.6 Network Bootstrapping Credentials

Network bootstrapping credentials (as shown in the first step of Figure 2-1) are credentials that the network onboarding component requires so the network can be authenticated by the device. Network bootstrapping credentials have to be provided to the network onboarding component before the onboarding process is initiated (assuming that the onboarding process requires the network to be authenticated by the device). As part of the onboarding process, the device will authenticate the network based on these network credentials. These network bootstrapping credentials may include information such as:

- network identifier (e.g., X.509 certificate, service set identifier [SSID])
- secret (e.g., private key)

To protect the secret from being disclosed, it should be safeguarded in a secure storage component to which the network onboarding component has access. If an onboarding solution does not require that the network be authenticated by the device, the network onboarding component does not need network bootstrapping credentials.

2.7 Device Information Declaration

In support of some onboarding solutions, an artifact may be needed that asserts information about the IoT device, which we call a *device information declaration*. Among the information asserted in the device information declaration could be the:

- certificate of the device owner
- certificates of all entities (if any) that the device owner has authorized to onboard the device (in addition to the device owner)

Creation and maintenance of the device information declaration is the responsibility of the device manufacturer (which is the first owner of the device) but could be delegated to another party, providing that party is trusted by both the network onboarding component and the device. As ownership of the device is transferred from one entity to another during the device life cycle, any ownership information that is present in the device information declaration has to be kept up-to-date, with each change of ownership clearly recorded. If the device owner wants to authorize entities other than itself to onboard the device, the owner would list these entities in the device information declaration. The owner could add or remove entities from this authorized onboarders list as needed during the device life cycle.

Support for a device information declaration (or similar mechanism) is optional. Not all manufacturers will create device information declarations for their devices, and not all devices will have associated device information declarations. To support security capabilities such as proof of ownership (Section 6.4.17) and to onboard only to authorized networks (Section 6.4.19), however, a device information declaration or similar mechanism will be needed.

The proof of ownership and onboarding only to authorized networks security characteristics enable an onboarding solution to assure an IoT device that the network that is trying to onboard it (and thereby take control of it) is authorized to do so. These mechanisms can help protect a device from being intercepted and taken over by a rogue network that attempts to onboard the device at some point before the device reaches its intended point of installation. If an onboarding solution includes a device information declaration or similar mechanism, the IoT device can consult the device ownership information (if present) in the device information declaration to determine whether the network that is trying to onboard it is owned by the device's owner. If so, this provides assurance that the device was acquired to be used on this network and indicates that such onboarding should be permitted. In other cases, if the network that is trying to onboard the device is not owned by the device's owner, the IoT device can consult the list of authorized onboarders of the device (if present) in the device information declaration to verify that the network that is trying to onboard it is owned by one of the entities that the device's owner has explicitly authorized to onboard it.

To be useful, the device information declaration has to be trusted by the entities that are consulting it, i.e., the IoT device and the onboarding component. Such trust could be established, for example, by having the device manufacturer sign the device information declaration or by ensuring that the device information declaration is available from a widely trusted, well-known server. As ownership or other information within the device information declaration changes, it needs to be updated and re-signed as appropriate.

In the first step of Figure 2-1, the device information declaration is depicted as being part of the bootstrapping process. One way that it could be used during bootstrapping would be for the device information declaration to have been signed by the device manufacturer and sent to the network owner upon purchase of the IoT device. Then, during bootstrapping, the network onboarding component could provide the device information declaration to the IoT device for the device to consult to determine whether the network is authorized to onboard it.

2.8 Network-Layer Versus Application-Layer Onboarding

The type of onboarding that we have discussed so far in this paper is network-layer onboarding (as shown in the first two steps of Figure 2-1). Onboarding can occur not only at the network layer but also at the application layer. To be functionally useful, most IoT devices undergo two different levels of onboarding: one at the network layer, which enables them to connect securely to the network; and one at the application layer, which enables them to become operational at the application layer. The subject of this paper is network-layer onboarding, but it is helpful to be explicit about the existence of application-layer onboarding (as shown in the fourth step of Figure 2-1) and distinguish it from network-layer onboarding, to avoid confusion. The term onboarding, when used alone in this paper, as defined in Section 2.1, refers to network-layer onboarding.

Network-layer onboarding is necessary to enable a device to connect to the network so it can communicate securely with the other entities on the network with which it needs to communicate to be part of the operational network. If a device needs credentials to be granted access to the cloud at the network layer, this provision will occur as part of network onboarding. That is, it is part of the process required to provide the device what it needs to enable it to communicate with other entities with which it needs to interact at the network layer.

Application-layer onboarding is necessary to enable the device to execute its primary function (i.e., to execute some sort of application-layer functionality). Application-layer onboarding (as shown in the fourth step of Figure 2-1) occurs subsequent to both network-layer onboarding and establishment of a secure network connection, because network-layer onboarding and secure network connection are the mechanisms that facilitate application-layer onboarding. Network-layer onboarding can support bootstrapping the application-layer onboarding process if application-layer bootstrapping information is included in the device's network-layer onboarding credentials. Recall from Section 2.2 that, in addition to the credentials that the device needs to securely connect to the network, the device's onboarding credentials may also include additional configuration information needed to enable the device to become operational at the application layer. If included, this additional information can bootstrap any application-layer onboarding process that may need to occur after the device has connected to the network. For example, this information could direct the device to a particular controller, server, or cloud service that, when contacted by the device, will securely install a necessary application on the device.

Once network-layer onboarding has occurred, the device may need to identify its owner or determine what entity it should trust to provision an application on it. This information could have been provided to the device as part of its onboarding credentials. The device can use the secure network-layer connectivity that it enjoys because of connecting to the network to establish trust and to secure channels with those other entities on the network as required. Those other entities (e.g., controllers or application servers) will provision the desired application-layer functionality to the device, thereby enabling the device to become operational at the application layer once it begins executing those applications. This application-layer functionality can include authentication/authorization with a cloud service, application provisioning, subscription to firmware updates, device ownership assignment, and device lifecycle management. For example, Amazon Web Service's IoT Device Management provides a number of application-layer services that allow IoT devices to be registered to an owner, track device attributes (such as device ID, status, and location), and deploy firmware updates to different devices. Other services like Microsoft's Azure IoT hub support a collection of device telemetry and allow custom message routing, IoT device simulation, and additional types of secure device communication using a variety of cipher suites.

3 High-Level Description of Onboarding

Earlier, we provided definitions of onboarding and related concepts. In this section, we provide a high-level description of the onboarding process in a solution-neutral manner. We describe the basic elements of the onboarding process that may occur when an IoT device is introduced to a media interface. This high-level description is intentionally general and includes generic phases in the device onboarding process. It may have aspects that are pertinent to some onboarding solutions but absent from others. For example, some onboarding solutions may support device authentication but not network authentication; some may support verification of device ownership, and some may not. Nevertheless, we include network authentication and device ownership verification steps in our description because these may be aspects of some onboarding solutions.

The steps that a device goes through to become operational can be viewed in terms of four general phases: pre-onboarding, network-layer onboarding, network connectivity, and application-layer onboarding. Because this paper focuses on network-layer onboarding, we detail only the pre-onboarding and network-layer onboarding phases in the subsections below. We summarize the pre-onboarding phase in Table 3-1 and Table 3-2, and we summarize the network-layer onboarding phase in Table 3-3.

The pre-onboarding phase occurs before the device is associated with any given network. The goal of the pre-onboarding phase is to equip the device and the network with their bootstrapping credentials (i.e., the information that each needs to be identified, authenticated and, in the case of some devices, associated with a MUD file) and to generate a device information declaration that will associate the device with a specific owner. The bootstrapping credentials and device information declaration will be used in the onboarding phase to enable the device and the network onboarding component to establish sufficient trust in each other to enable onboarding to take place.

The goal of the network-layer onboarding phase is to provision new credentials to the device—onboarding credentials, which will enable the device to securely connect to the network in question. Once the device has a secure network connection, the device can use the connection to perform application-layer onboarding, if needed. During application-layer onboarding, the application that the device needs to execute to perform its intended function is securely downloaded to the device. Once this application is downloaded and executed, the device becomes operational.

3.1 Pre-onboarding

The pre-onboarding phase consists of some activities that are relevant to the IoT device and other activities that are relevant to the local network.

3.1.1 Pre-onboarding at the IoT device

The activities of the pre-onboarding phase that are relevant to the IoT device typically occur as part of the manufacturing process before the device is acquired by its first post-production owner/user. It consists of four general steps, as summarized in the four rows of Table 3-1:

- A manufacturer or integrator provides the device with a chipset and related hardware and software needed to support onboarding, and the device's bootstrapping credentials are installed on the device.
- If the onboarding solution supports a device ownership verification capability (or similar mechanism), the manufacturer (or other trusted party) will create and sign a device information declaration that asserts:
    - the device's current owner (e.g., the manufacturer)
    - a list of entities (if any) that have been authorized to onboard the device (in addition to the owner) (e.g., integrators that will need to onboard the device to their networks as part of the production process)
- If the device has a MUD file, the MUD file will be created and posted to the appropriate URL that is provided in the device bootstrapping credentials.
- Once the identity of the device's next owner is known (typically upon device purchase), the manufacturer (or other trusted party) will update and sign the device information declaration identifying the device's next owner and any other authorized onboarders that that owner has designated.

Table 3-1 Summary of IoT Device-Related Pre-Onboarding Activities

Subphase	Activities	Example	Security Benefit
device bootstrapping credential provisioning	• Install onboarding-related chipset, hardware, and software on device. • Install bootstrapping credentials on device.	credentials such as a DevID, DICE CDI, private key or other secret, public/private key pair, MUD file URL, Wi-Fi channel that the device will use to communicate with the network onboarding component	enables device to be authenticated to the network onboarding component (identifier and secret), to express its intent (MUD file URL), and to inform the network onboarding component how to establish initial communications with it (Wi-Fi channel)
generate device information declaration	• Create the device information declaration. • Insert in it the owner's (i.e., the manufacturer's) certificate. • Insert in it the certificates of all the device's other authorized onboarders (if any). • Sign it.	The device information declaration is a signed digital assertion that is trusted due to its signature (or other mechanism) and that links the device with its owner. It may also specify other entities besides the owner (if any) that the owner has authorized to onboard the device.	This is trusted information that can be used by the device to ensure that the network that is trying to onboard it is authorized to do so (either because the network and the device have the same owner or because the owner of the device has explicitly authorized the network to onboard the device).

Subphase	Activities	Example	Security Benefit
MUD file posting	• Create and install the device's MUD file.	Post the device's MUD file to the URL listed in the device bootstrapping credentials.	enables the network to learn the device's intent so it can enforce appropriate device communications
update and transmit device information declaration	• Update the device information declaration to add the certificate of its next owner and certificates of newly designated authorized onboarders (if any). • Sign the device information declaration. • Send the device information declaration to the next owner and/or to all designated authorized onboarders.	The device information declaration is a trusted digital assertion that links the device with its next owner, thereby authorizing networks owned or authorized by that entity to onboard the device.	Keeps the device's owner and authorized onboarder information accurate and up-to-date and makes this information available to the device so that the device can refer to it to ensure that the network that is trying to onboard the device is authorized to do so

Figure 3-1 is a general four-step flow diagram of the IoT device-related pre-onboarding activities that take place at the manufacturer's site. Step one is installation of all onboarding-related chipsets, hardware, and software and of the device's bootstrapping credentials. This is the only pre-onboarding activity that is mandatory. If the onboarding solution will also support a proof-of-ownership verification capability, step two will be performed (i.e., the manufacturer will create the device information declaration to assert device ownership and perhaps designate authorized onboarders). If the device is MUD-capable (i.e., the URL of the device's MUD file was included in the bootstrapping credentials that were installed on the device during step one) and the onboarding solution supports conveyance of the MUD URL, step three will be performed. That is, the manufacturer will create and install the device's MUD file on the MUD file server.

Whether an onboarding solution supports MUD (Section 6.4.21) is independent of whether it supports proof of ownership (Section 6.4.17) and whether it can onboard only to authorized networks (Section 6.4.19). Therefore, it is possible that the pre-onboarding activities would include generation of the device information declaration but not creation of a MUD file, or vice versa, both, or neither. If the onboarding solution supports proof of ownership and/or MUD, however, ensuring that the device information declaration and/or the device MUD file remain up-to-date and available are ongoing responsibilities of the manufacturer (or trusted third party) that continue well beyond the manufacturing process until device end-of-life, and perhaps later.

The first three steps shown in Figure 3-1 can be performed when the device is manufactured. The fourth and last step, updating the device information declaration, cannot be performed until the identity of the device's next owner is known. Once this new owner is identified, the manufacturer can perform the fourth step to update and sign the device information declaration to ensure that it names the next owner and any authorized onboarders that that owner has designated. The manufacturer then transmits the device information declaration to the next owner of the device and possibly also to the authorized onboarders, if some have been designated.

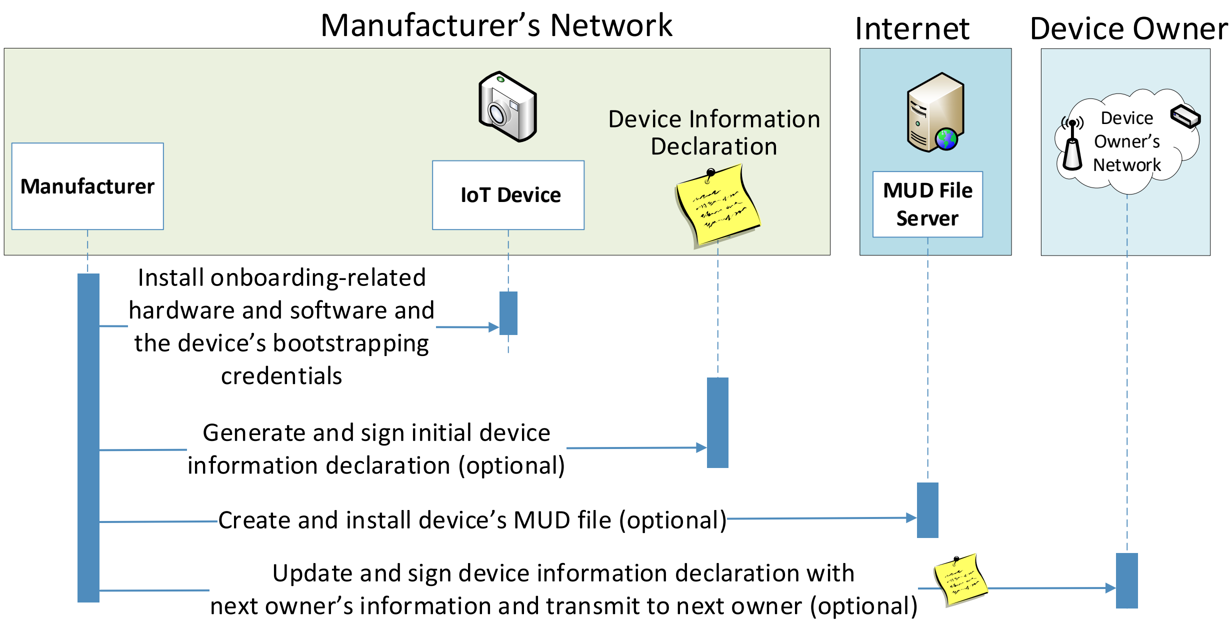

Figure 3-1 Pre-onboarding activities performed by the IoT device manufacturer

3.1.2 Pre-onboarding at the local network

In addition to the pre-onboarding activities that are performed by the manufacturer, the network owner may also be required to perform some pre-onboarding activities. If the onboarding process requires the network to authenticate to the device, the network owner performs the activity listed in the first row of Table 3-2: the network owner installs the network's bootstrapping credentials (e.g., the network's certificate and private key) on the network onboarding component. If network authentication is not required, this step is not necessary.

If the onboarding process supports a proof-of-ownership mechanism, the network owner performs both of the pre-onboarding activities shown in Table 3-2: both the network's bootstrapping credentials and the device information declaration are installed on the network onboarding component.

Table 3-2 Summary of Network-Related Pre-Onboarding Activities

Subphase	Activities	Example	Security Benefit
network bootstrapping credential provisioning	• Install the network's bootstrapping credentials on the network onboarding component.	credentials such as an X.509 certificate and private key. These will enable the IoT device to authenticate the network during the onboarding process.	enables the network onboarding component to be authenticated to the device
device information declaration provisioning	• Install the device information declaration on the network onboarding component.	assertion signed by manufacturer or other trusted party that identifies the device's owner and any designated authorized onboarders. It will be provided to the IoT device so the IoT device can be assured the network is authorized to onboard (i.e., take control of) the device.	provides the network onboarding component with trusted information it can give to the device to enable the device to verify the network is authorized to onboard the device

These two pre-onboarding steps (installation of the network's bootstrapping credentials on the network onboarding component, followed by installation of the device information declaration on the network onboarding component) are illustrated in Figure 3-2.

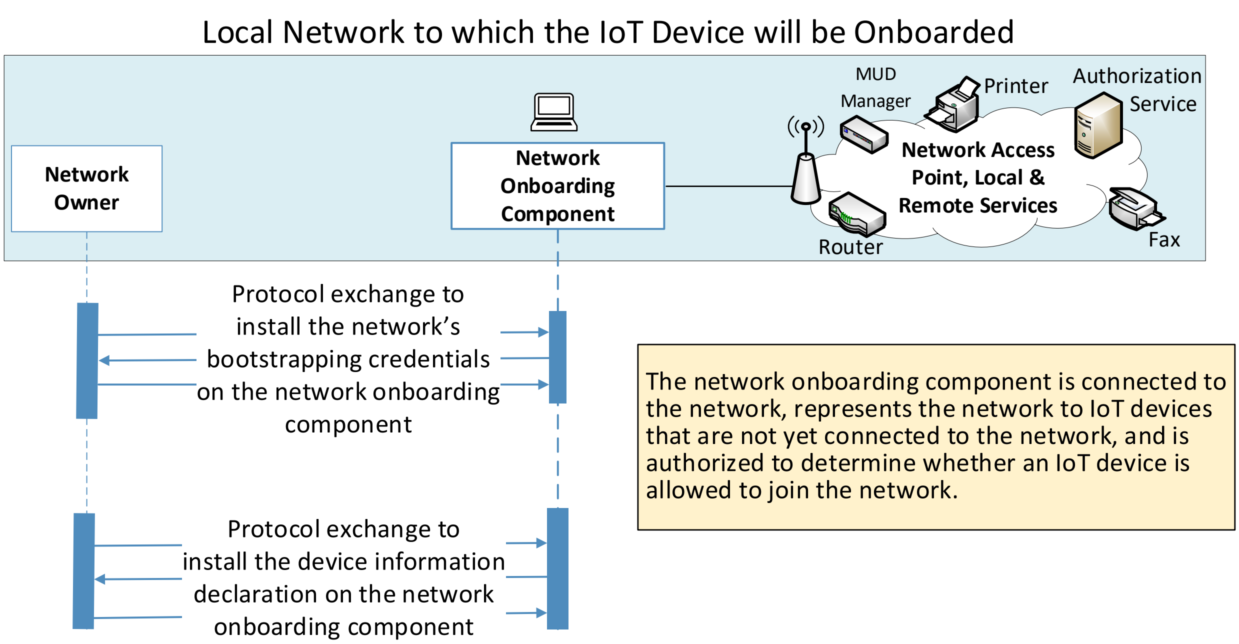

Figure 3-2 Pre-onboarding activities performed by the owner of the onboarding network

3.2 Network-Layer Onboarding

Because the device is not yet securely connected to the network at the time of onboarding, the device interacts with the network onboarding component. The device and the network onboarding component interact using an onboarding protocol. The onboarding protocol will be well defined, including specific messages for NIST-approved session establishment and cypher suites. The details of the onboarding protocol exchanges will be specific to the particular onboarding protocol used; in this section we describe those exchanges in a generic manner.

As discussed in Section 2, network-layer onboarding begins with the subprocess of bootstrapping. During bootstrapping, trust is established between the device and the network onboarding component of the network, and based on this trust, a secure channel is established. Once this secure channel between the device and the network onboarding component is established, the bootstrapping process is over. Onboarding then proceeds with this secure channel being used by the device to provide any information to the network that it wants to convey securely (e.g., its MUD URL) and by the network onboarding component to send the device its onboarding credentials, which include the credentials that the device needs to securely connect to the network.

In Table 3-3, all the rows except the last two describe elements of the bootstrapping process. The last two rows summarize the remainder of the onboarding process (i.e., using the secure channel to send the MUD URL to the network and to provision onboarding credentials to the device).

Bootstrapping can be understood in terms of the following steps, which correspond to the first eight rows of Table 3-3:

- For the device to be onboarded, it is placed in onboarding mode i.e., it enters a state of actively listening for onboarding protocol messages and being able to send onboarding protocol messages to the network onboarding component.
- The network onboarding component is provided with the device's bootstrapping credentials. These may be provided OOB. They may be provided manually by a trusted individual, or they may be provided by an automated process if the process is trusted.
- The device's bootstrapping credentials are propagated to the network so that it can be configured to expect the device. For example, if the network has an Authentication, Authorization, and Accounting (AAA) server or an authorization service, it will need to be configured to define what resources the device is authorized to access.
- If a device information declaration has been created for the device, the network onboarding component provides the device with the device information declaration. The device then uses the device information declaration to ensure that the network has been authorized to onboard it. If there is no device information declaration for the device, the device cannot verify whether the network has been authorized to onboard it.
- The network onboarding component authenticates the device.
- The device authenticates the network onboarding component.

- A secure channel is established between the device and the network onboarding component.
- If the device has a MUD file, its URL, which is specified in the device's bootstrapping credentials, is conveyed to the network. The network MUD manager retrieves the device's MUD file and uses it to configure the network router to enforce the device's communications profile as defined in the device's MUD file.

The first three steps (when the device is put in onboarding mode, its bootstrapping credentials are provided to the network onboarding component, and the device is registered with the network) may be performed out of band via manual interaction. However, the remaining steps (retrieval and use of the MUD file, transmission of the device information declaration to the device, authentication of both the device and the network, and establishment of a secure channel between the device and the network onboarding component) are automated processes supported by the onboarding protocol.

Also, as was mentioned earlier, not all steps listed above necessarily occur in all onboarding solutions. Some onboarding processes may require only one-way rather than mutual authentication between the device and the onboarding component; some IoT devices may not have an associated MUD file, and some devices may not have a device information declaration. In these cases, the corresponding steps would be omitted from the bootstrapping process. Also, the steps may not necessarily occur in the exact order stated above. For example, some onboarding solutions may not send the device's MUD file URL and retrieve the device's MUD file until after the device has been authenticated.

Note also that a given onboarding solution can be designed to work with a variety of different bootstrapping mechanisms, some of which may be considered more trustworthy than others. The bootstrapping mechanism that is chosen for use in any given application of the onboarding solution will play a significant role in determining the overall level of security assurance that the onboarding solution can provide.

The bootstrapping process is complete once a secure channel is established between the device and the network onboarding component. The network-layer onboarding process is complete once the network onboarding component has used this secure channel to receive the device's MUD file URL (if supported) and any other necessary information that it has not already received and to send the device its onboarding credentials (i.e., at a minimum, the information that the device needs to securely connect to the network).

695 **Table 3-3 Summary of IoT Device Network-Layer Onboarding**

Subphase	Activities	Example	Security Benefit
Put the device in onboarding mode.	• The device is powered on so that it can communicate with the network onboarding component, and it begins either transmitting or listening for onboarding protocol messages.	The device is using the appropriate Wi-Fi channel (if using wireless access), it is connected to the onboarding component (if using wired access), and it is generating/listening for onboarding protocol messages.	enables device to begin communicating with the network onboarding component
trusted introduction of device bootstrapping information to the network onboarding component	• Provide the network onboarding component with the information it needs to communicate with and authenticate the device. The information may be provided OOB. It may be provided manually by a trusted individual or directly from the device if the device has a hardware root of trust.	Information will typically include most of the device bootstrapping credentials (e.g., X.509 certificate or device ID and public key, Wi-Fi channel, communications protocols, and related parameters). It will not include the device's secret.	provides the network onboarding component with trusted information that it can use, .e.g., to authenticate the device and know how to establish initial communications with the device
Register the device with the network.	• Provide the device information to the local network (e.g., provide the device identity to the authorization service so the network will be expecting the device and the device's authorizations can be configured).		enables authorization information to be associated with the device
transmission of device information declaration to the device	• The network onboarding component provides the device with the device information declaration. • The device uses the device information declaration to ensure that the network is authorized to take control of (i.e., onboard) it. • If the onboarding solution does not support proof-of-ownership verification, this step would not be performed.	The network onboarding component will provide the device with the network information declaration (a signed assertion of device ownership) or with the network's certificate or other credential if the onboarding solution does not support proof-of-ownership verification.	provides the device with trusted information that it can use to ensure that the network that is trying to onboard it is authorized to do so (either because the network and the device have the same owner or because the owner of the device has explicitly authorized the network to onboard the device)

Subphase	Activities	Example	Security Benefit
Put the device in onboarding mode.	• The device is powered on so that it can communicate with the network onboarding component, and it begins either transmitting or listening for onboarding protocol messages.	The device is using the appropriate Wi-Fi channel (if using wireless access), it is connected to the onboarding component (if using wired access), and it is generating/listening for onboarding protocol messages.	enables device to begin communicating with the network onboarding component
device authentication	• device presents its bootstrapping credential to the network onboarding component, which authenticates the device	The network uses the device's public key to authenticate the device.	enables the network onboarding component to ensure that the device has the identity that it claims to have
network authentication	• The network onboarding component presents its credentials to the IoT device, which authenticates the network.	The device uses the network's public key and the device information declaration to authenticate the network and ensure that it is authorized to take control of the device.	enables the device to ensure that the network onboarding component has the identity that it claims to have; and if the device has a device information declaration, consulting it enables the device to ensure that the network is authorized to onboard the device
secure channel establishment	• The device and the network onboarding component establish a shared secret key to encrypt subsequent exchanges.	The device and the network perform a Diffie-Hellman (or similar) exchange of cryptographic keys, based on the secrets in their bootstrapping credentials.	This secure channel, which, preferably, has a unique, one-to-one binding between the device and the onboarding component, ensures confidentiality of the device's onboarding credentials while they are in transit between the network onboarding component and the device.
device sends network its MUD file URL	• The device sends the network onboarding component its MUD URL over the encrypted channel.		enables device intent information to be strongly associated with the device
Retrieve device's MUD file and configure its access rules on the network router.	• Retrieve the device's MUD file based on the MUD URL in the device bootstrapping credentials. • Configure the network router to enforce the MUD file access rules for the device. • If the device does not have an associated MUD file, this step would not be performed.		enables the network to understand and enforce the device's communications intent, as expressed in its MUD file
device onboarding	• The network onboarding component provisions the device	The device's network credential	provides the device with the unique credentials it needs

Subphase	Activities	Example	Security Benefit
Put the device in onboarding mode.	• The device is powered on so that it can communicate with the network onboarding component, and it begins either transmitting or listening for onboarding protocol messages.	The device is using the appropriate Wi-Fi channel (if using wireless access), it is connected to the onboarding component (if using wired access), and it is generating/listening for onboarding protocol messages.	enables device to begin communicating with the network onboarding component
credential provisioning	with the onboarding credentials it needs to connect to the network (e.g., SSID and a PSK). • The network onboarding component may also provision the device with information it will need to bootstrap application-layer onboarding once it has connected to the network.	can be a PSK, simultaneous authentication of equals password, connector, or other secret that is, preferably, unique to the device. The application-layer bootstrapping information provisioned to the device may indicate what controllers, application servers, cloud services, and other components the device should contact to perform application-layer onboarding and become operational at the application layer.	to establish a secure connection with the network and, optionally, with additional information that will enable the device to eventually be securely provisioned with application-layer functionality

Figure 3-3 is a general flow diagram of the onboarding process. It begins with the device being put in onboarding mode and the trusted introduction of device bootstrapping credentials to the network onboarding component. This introduction may be performed out of band and may require human interaction. Regardless of the mechanism, introduction of this information occurs via a mechanism that is trusted. Also, in onboarding solutions that include support for proof-of-ownership verification, the network onboarding component will have already been provided with the device information declaration, and it will transmit this declaration to the IoT device for the device to use to verify that the network is authorized to onboard it.

After the network onboarding component receives the device bootstrapping credentials, information about the device is provided to the rest of the network as a way of enabling the device to be registered on the network. Depending on the situation, operations based on the device information may be performed on the network. For example, the authorization service can be configured with information regarding what network resources the device is authorized to access.

As shown in Figure 3-3, once the network has been configured to expect the device, the device authenticates itself to the network and, if required, the network authenticates itself to the device. Each of these authentications requires a series of protocol exchanges that involve the entity that is being authenticated using its bootstrapping secret to demonstrate that it is whom it claims to be, by virtue of being in possession of this secret. When the network authenticates itself to the device, the device will also use information in the device information declaration to ensure that the network is authorized to onboard the device, and it will use the network's certificate and public key to ensure that the network has the identity that it claims to have. The details of the protocol exchanges that need to occur to perform this authentication are specific to the onboarding protocol used. After both the device and the network onboarding component have been authenticated, the device and the network onboarding component establish a secure channel. Assuming the device is MUD-capable and the onboarding solution supports transmission of the MUD file URL, the device will use this secure channel to provide its MUD file URL to the network onboarding component. The network onboarding component can then forward the MUD file URL to the MUD Manager, which retrieves the device's MUD file and uses it to configure the network router to enforce the device's communications profile. The network onboarding component then uses the secure channel to provision the device's onboarding credentials to the device.

Because this flow diagram is meant to be general, it may contain components or steps that are not in all onboarding situations. For example, not all devices will have a device information declaration, and not all devices will have an associated MUD file. Without having a specific onboarding solution in mind, it is not possible to depict the exact protocol exchanges that would take place. Nor is it possible to know in what order the device and network authentication would be performed. This flow diagram attempts to be as general as possible in providing an overview of the process, while also trying to keep the steps simple. For example, it assumes that the device being onboarded is MUD-capable, so it depicts the steps of retrieving the device's MUD file and installing its MUD rules on the router. Not all devices being onboarded will be MUD-capable, in which case the MUD-related steps depicted would not be performed.

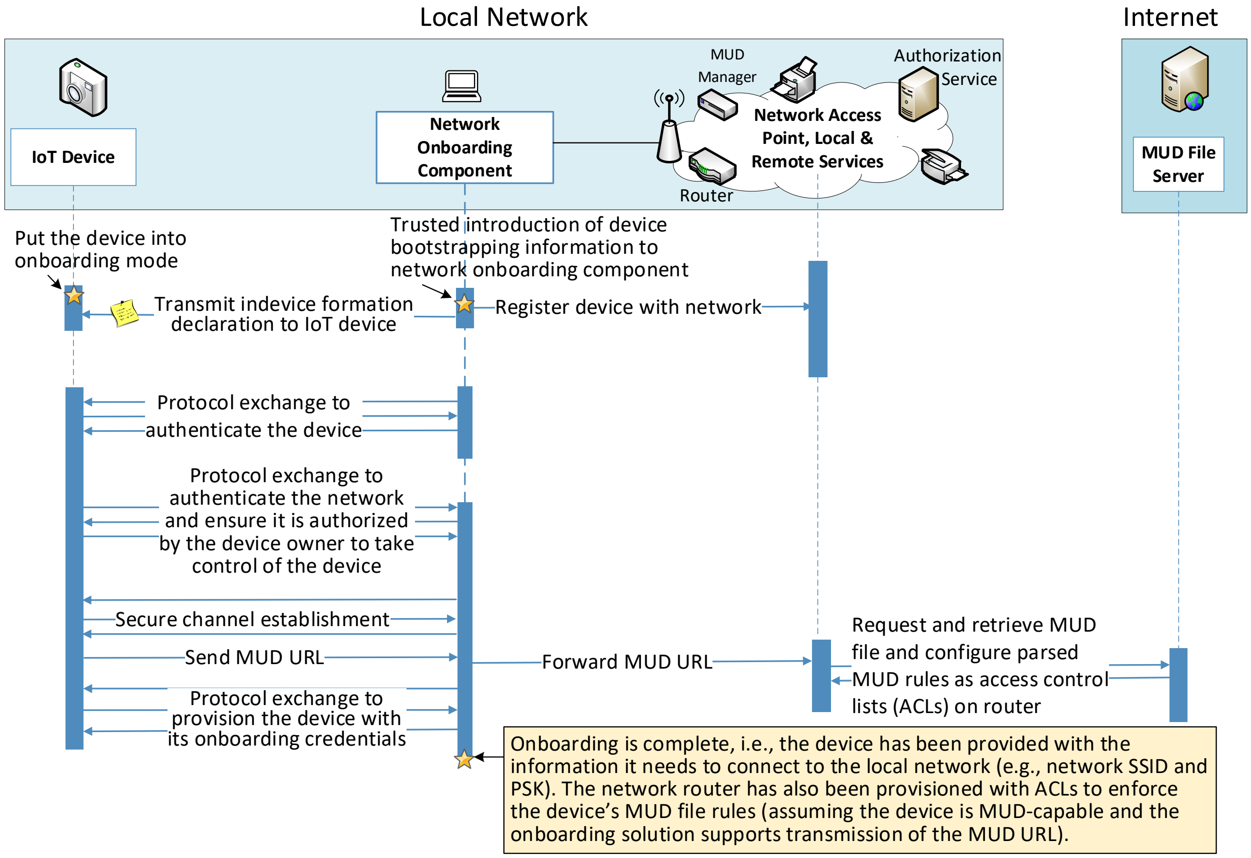

Figure 3-3 Flow diagram illustrating the general network-layer onboarding process

Once network-layer onboarding is complete, the device is no longer in onboarding mode. It is no longer listening for or generating onboarding protocol messages. It can connect directly to the network (rather than to the network onboarding component) by presenting its newly provisioned network-specific credentials to establish secure network associations. Once the device is connected to the network, it may perform application-layer onboarding by using application-layer bootstrapping information that may have been provided within its network-layer onboarding credentials. While the device is commissioned (see Section 4 for a description of the device's lifecycle phases), the network onboarding component and the onboarding protocol are no longer active or used. However, if the device needs to be provisioned with different onboarding credentials, due to events that affect its current credentials (e.g., credential expiration, security updates, key rotation, or certificate renewals) or due to the device being repurposed or resold, then the device's current onboarding credentials would be deleted and the device would be placed in onboarding mode so it could be re-onboarded with the new credentials it requires.

In some onboarding situations, immediately after the device successfully connects to the network it may be desirable for the device to report this fact back to the network onboarding component as a diagnostic feature so the network onboarding component can be aware of the status of the device. In this case, there would be a brief period during which the device would communicate with the network onboarding component after the device has connected to the network.

3.3 Critical Information

Regardless of the onboarding solution, there is a collection of information on which the onboarding process relies. This information includes:

- device bootstrapping credentials concerning the device that are conveyed to the network onboarding component via a trusted introduction (assuming the device is to be authenticated to the network)
- network bootstrapping credentials concerning the network that are provided to the device that is being onboarded (assuming the network is to be authenticated to the device)
- ownership and authorized onboarder information (if any) in the device information declaration (assuming the device is to verify that the network that is trying to onboard it is authorized to do so)

This is the information conveyed in the first row of Table 3-1 and in the first two rows of Table 3-2. For any given onboarding solution, the type and amount of the information that is conveyed to the device and to the network onboarding component will depend on the characteristics of that onboarding solution (see Section 6). To ensure that they will be able to accommodate all onboarding solutions, the data structures that are defined to convey this critical information should be designed to include fields that accommodate all information needed to support the onboarding characteristic enumerated in Section 6. In addition, the data structures should be defined to be extensible so they can accommodate information for which the need may not yet be envisioned. Ideally, all stakeholders should try to define and standardize the data structures and a list of fields and ensure that they are comprehensive enough to convey all information that is necessary to support any given onboarding solution. The information conveyed should either be provided or signed by an entity that the recipient trusts.

The voucher artifact defined in Request for Comments (RFC) 8366 [9] provides an example structure that instantiates information needed to support trusted bootstrapping mechanisms. It most closely resembles the information conveyed in a device information declaration. A device's manufacturer would generate and sign the voucher defined in RFC 8366, enabling the voucher to securely associate the device with its owner. The device can use this voucher to determine if the network that is trying to onboard it also belongs to its owner, under the assumption that the device should allow only its owner's network to take control of it. The network onboarding component would receive this voucher from the device manufacturer and pass the voucher to the IoT device so the IoT device could authenticate the network onboarding component and determine if it should allow itself to be onboarded to the network. The voucher includes an X.509 root certificate that enables the device to authenticate the network onboarding component's identity. The voucher artifact defined in RFC 8366 is used by several bootstrapping protocols currently in development, such as Zero Touch Provisioning for Networking Devices, 6TiSCH Secure Join protocol, and Bootstrapping Remote Secure Key Infrastructure. It is defined as a JavaScript Object Notation (JSON) object and expressed as a Yet Another Next Generation model, which provides standard properties to describe the object.

4 Onboarding Lifecycle Management

Lifecycle management refers to the operations that are performed to manufacture, configure, secure, use, update, and otherwise manage IoT devices and their credentials through all phases of the devices' existence. Ideally, all aspects of lifecycle management should be performed securely. Figure 4-1 depicts a high-level overview of the life cycle of a generic IoT device with a focus on the various aspects of the life cycle related to onboarding. This diagram and the definitions of the lifecycle phases it depicts are informed by [10], [11], [12], and [13].

Not all devices will experience all the phases and events in this generic life cycle or in the more detailed depictions of it that are provided later in this section. The specific phases and operations that pertain to a given device depend on the purpose of the device, the context of its deployment use case, and any specific circumstances that may arise.

Note that in our discussion of the IoT device life cycle, we use the term *supply chain* different from how it is defined in National Institute of Standards and Technology (NIST) Special Publication 800-161 [14]. That document defines the supply chain as encompassing the entire scope of the software development life cycle, from research and development through transportation, acquisition, deployment, use, operations, and maintenance to retirement. In this paper, the scope of the term supply chain is more constrained. As used in this paper, the supply chain also begins at research and development, but it extends only to the point at which the device is acquired by its first post-manufacturing owner. For purposes of the lifecycle management discussion in this paper, the supply chain is not understood to include the period in which the device is installed, onboarded, commissioned, used, maintained, decommissioned, or retired.

At the highest level, the device life cycle as we define it consists of two general phases: a supply-chain phase and a use phase. While in its supply-chain phase, the device is, among other things, manufactured and shipped. While in its use phase, the device is, among other things, installed, onboarded, and commissioned; it cycles through periods of maintenance and operation and is ultimately decommissioned, at which point it may be either reinstalled elsewhere for further use or considered to have reached end-of-life. Both phases and subphases within them are described more fully in the following subsections.

Although onboarding is only one (possibly recurring) phase in the device life cycle, the onboarding mechanism may impact and be impacted by numerous other phases in the device life cycle. It is important to understand how onboarding affects and is affected by the various phases of the device life cycle to ensure that any onboarding solution being considered for use adequately integrates with and addresses all aspects of the device life cycle.

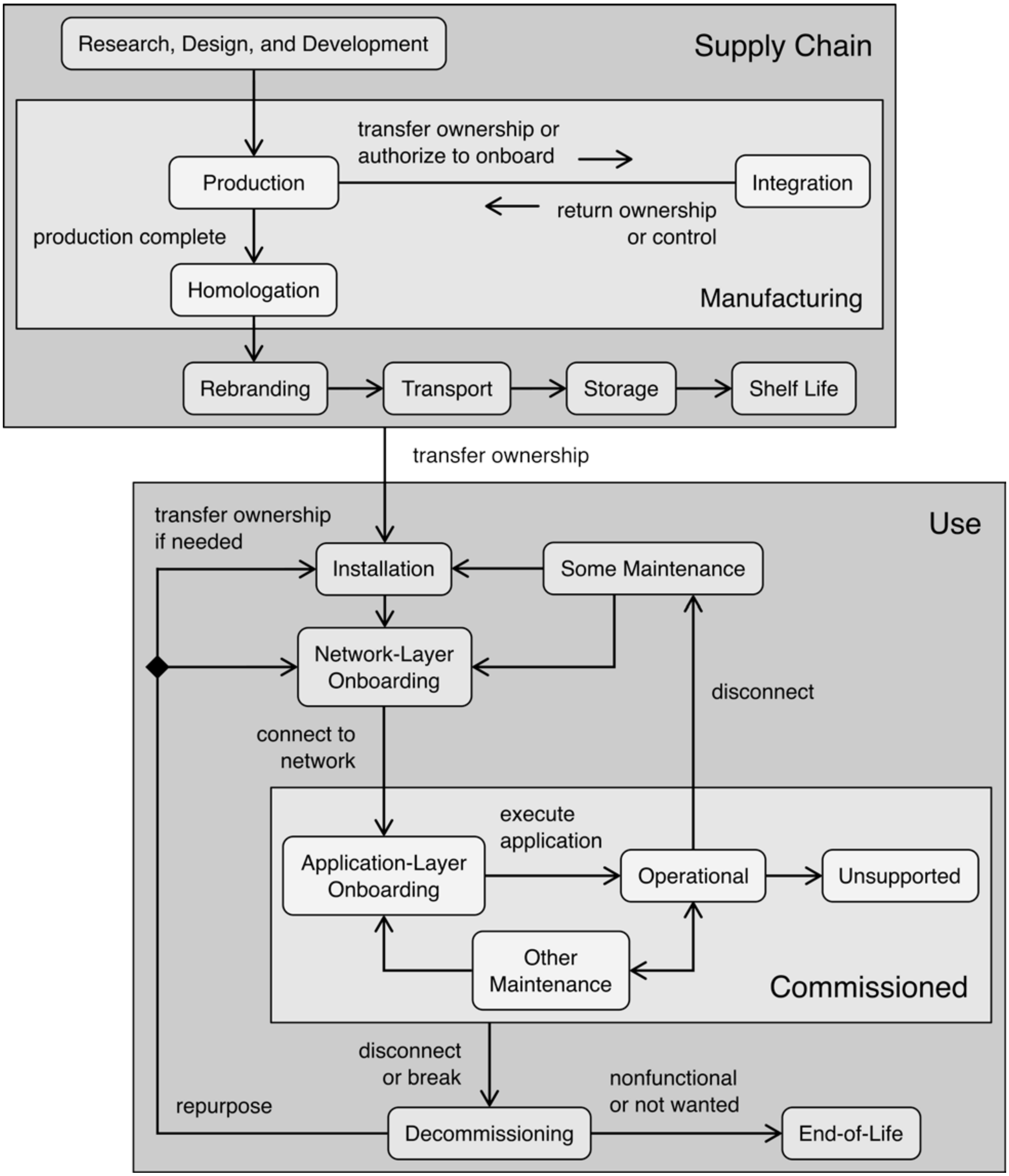

Figure 4-1 High-level overview of the IoT device life cycle from an onboarding perspective

4.1 Supply chain

Figure 4-2 provides a more detailed depiction of the first part of the IoT device life cycle: supply chain, with a focus on those aspects that are significant to the device's interaction with the network and, in particular, onboarding.

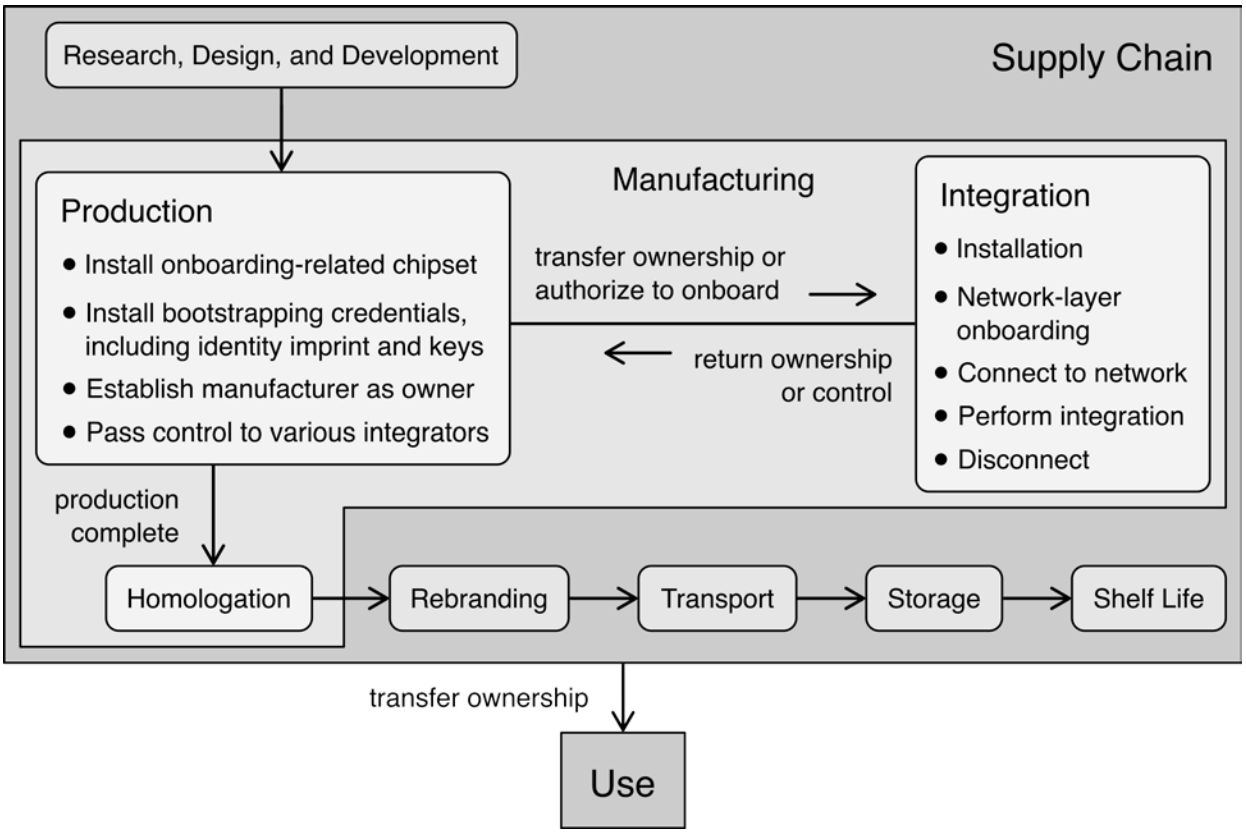

Figure 4-2 Supply chain phase of the IoT device life cycle from an onboarding perspective

As shown in Figure 4-2, the following phases and events may be part of the supply chain:

- Research, Design, and Development–This phase includes activities such as defining device requirements (including security and onboarding requirements), design, testing, trial and error, refinement, embedded security, and trial production runs for review and improvement. It is during this phase that decisions that affect the security and operation of onboarding may be finalized.
- Manufacturing–This is the phase during which the device is produced and assembled. It could involve not just in-house device production but also integration with components supplied by various part manufacturers, including installation of open-source or other software on the device. During the manufacturing phase, all onboarding-related hardware, firmware, and chipsets are installed, including a security hardware module or hardware root of trust, random number generator, or other components that may be

required. The device's identity is imprinted; its other bootstrapping credentials, such as private keys, are installed; and the manufacturer is established as the device owner. In onboarding solutions that support proof-of-ownership verification, the device information declaration will be created to list the manufacturer as the device owner and, if supported, it will also list all entities that the owner has authorized to onboard the device (e.g., integrators that will need to onboard the device to their networks as part of the manufacturing process, if any). Once production of the device is complete, just before leaving the manufacturing phase, the device is certified as being compliant with relevant homologation requirements.

- Integration–Integration is a subphase of the manufacturing phase. As part of the manufacturing process, the device may have to pass through a succession of system integrators, and some or all of those system integrators may need to connect the IoT device to their own networks for the short time necessary to install and integrate the desired component. When the device is passed to an integrator, it enters the integration phase. Once installed, onboarded, and connected to an integrator network, the device becomes operational only for undergoing the specific integration process required by that integrator. It is then disconnected from the integrator's network, and control (and possibly ownership) of the device is passed back to the manufacturer. The manufacturer may onboard it to its network for further production or pass it to another integrator, which onboards the device to its network, and so on, until all system integration is complete and the device is ultimately transferred back to the manufacturer.

  For the integrator to onboard the device to its network, the integrator needs to be either the owner or an authorized onboarder of the device. Ideally, the mechanisms used to transfer the device from the manufacturer to a succession of system integrators for onboarding on their networks will not need to be different from those used to repurpose an older device that is sold to a new user after a period of use by its original owner. Assuming the onboarding solution supports a proof-of-ownership verification mechanism (Section 6.4.17), the manufacturer could support the system integration process by using the device information declaration to formally transfer ownership of the device back and forth between the manufacturer and a succession of system integrators (see the next point, Transfer Ownership). If the onboarding solution also supports an "onboard only to authorized networks" mechanism (Section 6.4.19), then instead of the manufacturer having to transfer ownership back and forth between itself and various integrators, the manufacturer could use the device information declaration to formally designate each system integrator to be an authorized onboarder of the device (see two points down, Grant Authorization to Onboard). The device may continue to loop through a succession of integration subphases, depending on how many integrators are involved in its manufacture, until production is complete. Once production is complete, the device is certified as compliant with relevant homologation requirements, and it leaves the manufacturing phase to continue through its life cycle.

    - Transfer Ownership–This is an event rather than a phase in the device life cycle. A device's owner may initiate an ownership transfer event for the device either before the device has been onboarded or after the device has been decommissioned but not during the period in between. Just prior to the ownership transfer event, the current owner should delete all information on the device except the device's bootstrapping credentials. In addition, if the onboarding solution supports proof-of-ownership verification or similar capabilities, the new ownership information (and perhaps authorized onboarder information, if supported) needs to be inserted in the device information declaration, which would then be re-signed. A device may have only one owner at a time.
    - Grant Authorization to Onboard – This is also an event rather than a phase in the device life cycle. A device's owner may initiate this event at any point in the device life cycle, assuming the onboarding solution supports it. As part of this event, the device information declaration will be updated with the list of entities that the owner has authorized to onboard the device, and then it will be re-signed.
- Rebranding–This phase may occur if a device is rebranded by a vendor other than the original manufacturer. If the device supports mechanisms such as a device information declaration that tracks device attributes such as ownership and authority to onboard the device, or a MUD file that describes the device's communications profile, the responsibility for maintaining the MUD file or the device information declaration may be securely passed from the manufacturer to the vendor that has rebranded the device.
- Transport–This is the phase in which the device moves from the manufacturer to and among other locations (e.g., integrator facilities, warehouses, retail locations) for integration, storage, branding, or other purposes until the device reaches its first post-production owner. A device may enter this phase several times as it moves between other phases and subphases, depending on the geographic location of the device's manufacturer, integrators, rebrander, warehouses, and retail locations.
- Storage–This is the phase during which the device is kept in a warehouse or other storage facility before it reaches a retail location or its first owner.
- Shelf Life–This phase occurs after the device has been manufactured but before it is purchased and installed by its first post-production owner. The device sits on the shelf in a retail location, waiting to be acquired. All phases of the device life cycle through this phase are considered part of the device's supply chain, according to the limited definition of that term that we are using in this document. Note that if the device bootstrapping credentials were to expire during this phase, the storage phase, or at any other time, trusted onboarding as we envision it would not be possible. This demonstrates why, as stated in Section 2.5, if the device bootstrapping credentials include a certificate, that certificate should not expire.

4.2 Device Use

Once the device is acquired by its first post-production owner, it leaves the supply chain and enters its use phase. Figure 4-3 shows a detailed depiction of this portion of the device life cycle, once again with a focus only on the device's interactions with the network and those aspects that are significant to onboarding.

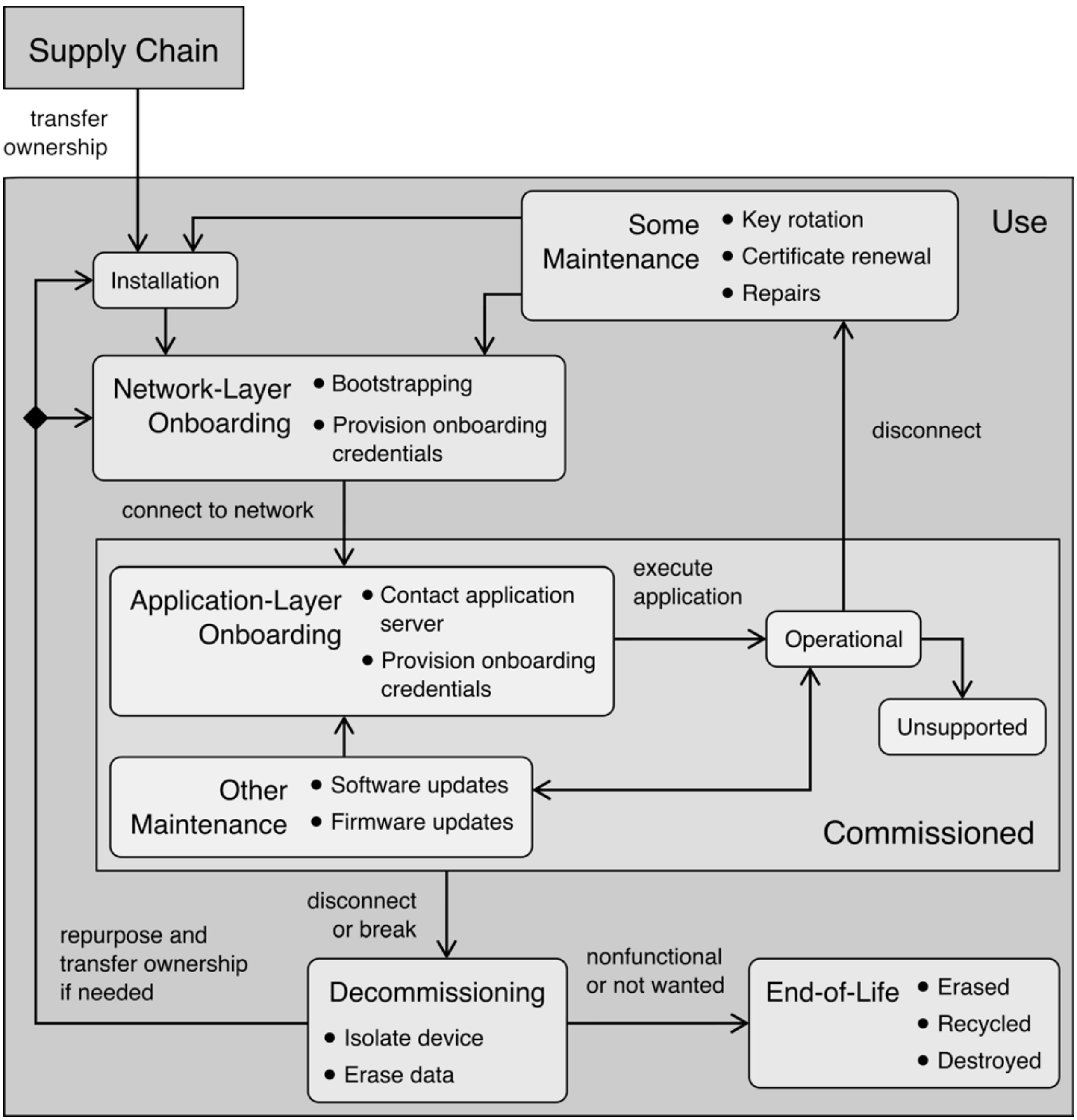

Figure 4-3 Use phase of the device life cycle from an onboarding perspective

As shown in Figure 4-3, the following phases and events occur after the device has left the supply chain portion of its life cycle, during its period of use:

- Installation–This is the phase during which the device is physically placed into position, turned on, and, if it will have wired network access, physically connected to the network. If any buttons need to be pushed, antennae need adjustment, or the device needs to otherwise be prepared for onboarding, those operations are performed as part of the installation. (In some deployments, the installation phase may be performed after network-layer onboarding rather than prior to it. For example, in some deployments, an IoT device is required to be sealed underground or elsewhere and not accessed for many years. In these deployments, it would make sense to perform onboarding before installation, if possible, to ensure that onboarding was successful before sealing the device away.)
- Network-Layer Onboarding–Network-layer onboarding is defined in Section 2.1. During this phase, device bootstrapping (defined in Section 2.4) occurs, after which the device is provided with its onboarding credentials—i.e., the information it needs to connect to the network (e.g., the identity of the network and the device's network password) in a manner that is trusted. As part of the onboarding process, the device may be personalized with an identifier by the network owner (i.e., a device name that is meaningful to the network owner). The onboarding credentials provided to the device may also include application-layer bootstrapping information about any servers or controllers to which the device should securely connect for the eventual application-layer onboarding that is needed to enable it to perform its intended function.
- Connect to Network–Network connection is performed to transition the device from the network-layer onboarding phase to the commissioned phase.
- Commissioned–In this phase, the device enters secure connection to the network. Once commissioned, the device is operational at the network layer, meaning that it can communicate securely with other devices on the network.
- Application-Layer Onboarding–Application-layer onboarding is defined in Section 2.8. The device enters this phase immediately after being connected to the network. Once the device is commissioned, its goal is to begin executing the application-layer functionality that is necessary for it to perform its intended purpose. In some cases, the device's application may already be installed on it, in which case the device may begin fulfilling its intended purpose merely by executing its application. In other cases, the device's application may still need to be installed. In these cases, the onboarding credentials that were provisioned to the device may have included application-layer bootstrapping information (e.g., the URLs of servers or controllers that the device should trust to provision application-layer functionality to it) that the device needs to perform application-layer onboarding. In the application-layer onboarding phase, the device establishes a secure communications channel with the identified trusted application servers and controllers and permits those controllers and servers to use that channel to install the required applications on the device. Once those applications are installed, the device is assumed to have all applications it needs to function as intended and fulfill its purpose.
- Execute Application–This action may be invoked automatically after application-layer onboarding or by an application manager. It causes the device to begin executing its

intended application-layer functionality. Initiation of the device's application transitions the device from the application-layer onboarding phase to the operational phase.

- Operational–In this phase, the device's application is executing as intended; the device is performing its intended purpose.
- Maintenance–Maintenance phases may occur periodically and interrupt a device while it is in operational mode. Many different types of maintenance may be required—from routine updates to unexpected repairs due to device malfunction, compromise, age, or other factors. During a maintenance phase, the device is not operational. In describing the device's life cycle, Figure 4-3 depicts two general types of maintenance:
    - Some types of maintenance require the device to be disconnected from the network and possibly even uninstalled (e.g., replacement of security keys, certificate renewals, encryption library updates, some security patches or upgrades, and some physical repairs). After this type of maintenance is complete, the device may need to be reinstalled, and it will have to go through network-layer onboarding again, be reconnected to the network, and go through application-layer onboarding before returning to the operational phase.
    - Other types of maintenance can be performed while the device, though not operational, is still commissioned on the network (e.g., some software or firmware updates or security patches). After this type of maintenance is complete, the device may be able to transition directly back to the operational phase, or, if the maintenance involved patches, upgrades, or reconfiguring the device's application, the device may need to go through application onboarding again before returning to the operational phase.

  Once operational again, the device may continue to loop through the operational and various maintenance phases for some time until it is decommissioned.
- Unsupported–In some cases, the device may enter the unsupported phase. That is, it may be functional but is no longer supported by its manufacturer or one or more of the manufacturer's integrators (either because the manufacturer or integrator has gone out of business or because either the manufacturer or integrator has decided to stop supporting a device that has been deprecated), so the device stops looping through maintenance phases and moves to the unsupported phase. In this phase, the device is still operating on the network and executing its application despite that it may have unpatched, known vulnerabilities and is no longer covered under the manufacturer support contract. An unsupported device stays in the unsupported phase either until it is explicitly disconnected from the network, at which time it should be decommissioned, or until it breaks, at which time it needs to be decommissioned and will reach end-of-life by virtue of no longer being functional.
- Disconnect–The device manager does this to remove the device from the network so the device can be either maintained or decommissioned.
- Break–This results in the device no longer being functional. A device that becomes nonfunctional and is beyond repair needs to be decommissioned and will reach end-of-life.

- Decommissioning–During this phase, the device and application managers perform the operations needed to ensure that the device permanently stops performing its intended function on the local network. A device manager may decide to decommission a device if it stops functioning (e.g., breaks) and cannot be repaired or when it is determined that the device should no longer be used to perform its intended function on the network (perhaps due to becoming out-of-date or obsolete or losing software support). A device that has been decommissioned may be replaced on the network by a newer-model device. The decommissioning phase includes disconnecting and isolating the device so that it can no longer affect the network. It also involves erasing all sensitive data from the device, including application-related data (e.g., all onboarding information, logs, and user data that has been collected) so that the only information that is left on the device is its original bootstrapping credentials. A factory reset may be required to ensure removal of the desired information. After a device has been decommissioned, it may either reach end-of-life or be repurposed.

  It should be noted that there is a distinction between a device being decommissioned and reaching end-of-life in terms of its network connectivity and a device being decommissioned and reaching end-of-life in terms of its real-world functionality. Figure 4-3 depicts only the device's life cycle in terms of its network connectivity. A device that is decommissioned from the network may continue to be used while disconnected. For example, a connected washing machine may reach the end of its software support, leading its owners to disconnect it from the network and decommission it (in terms of network connectivity) so that it will not be vulnerable to a network-based attack due to unpatched software. This decommissioned device may still function well as a washing machine and may continue to be used to wash clothes. In terms of the decommissioned device's interaction with the network, however, it has reached end-of-life because it will not be used to connect to a network again.
- End-of-Life–This is the phase that a decommissioned device enters if:
  - The device is nonfunctional and cannot be repaired.
  - The device is functional but is no longer deemed useful for any purpose, not even on a secondary market.
  - The device will not be connected to a network again; it no longer needs those components it uses to interact with the network.

  Upon reaching end-of-life, a device should have all its sensitive data removed (to the extent possible), and it (or at least the components it uses to interact with the network) should be destroyed. Some of its parts (precious metals, batteries) may be recycled for use elsewhere.
- Repurpose–A device manager does this on a decommissioned device that is still usable in terms of interacting with a network. Repurposing means putting a device to a different use. It may be put to a different use by its current owner, or it may be sold on a secondary market and used by a new owner. When the device is repurposed, it essentially loops back to an earlier phase and begins proceeding through a new path in its life cycle.

  - If the device is remaining with its current owner but needs to be onboarded to a new network, it will loop back to the installation phase and then proceed through its life cycle.
  - If the device is remaining with its current owner and will be used on the same network but in a different role, the device will loop back directly to the network-layer onboarding phase and then proceed through its life cycle.

  If the device will be sold to a new owner, the current owner will execute an ownership transfer event before repurposing the device, assuming the technology supports this feature. After its ownership has been transferred to its new owner, the device will loop back to the installation phase and then proceed through its life cycle on a different network—one that belongs to or is authorized by its new owner. After being repurposed, the device will proceed through various lifecycle phases as it did before—perhaps looping through the operational and maintenance phases for some time, perhaps being repurposed one or more times—before ultimately reaching end-of-life.

Figure 4-4 summarizes the information provided in this section. It provides a comprehensive depiction of the complete IoT device life cycle, both the supply chain phase and the use phase. It provides a detailed depiction of all lifecycle subphases and events discussed in this section, with a focus on their significance to onboarding.

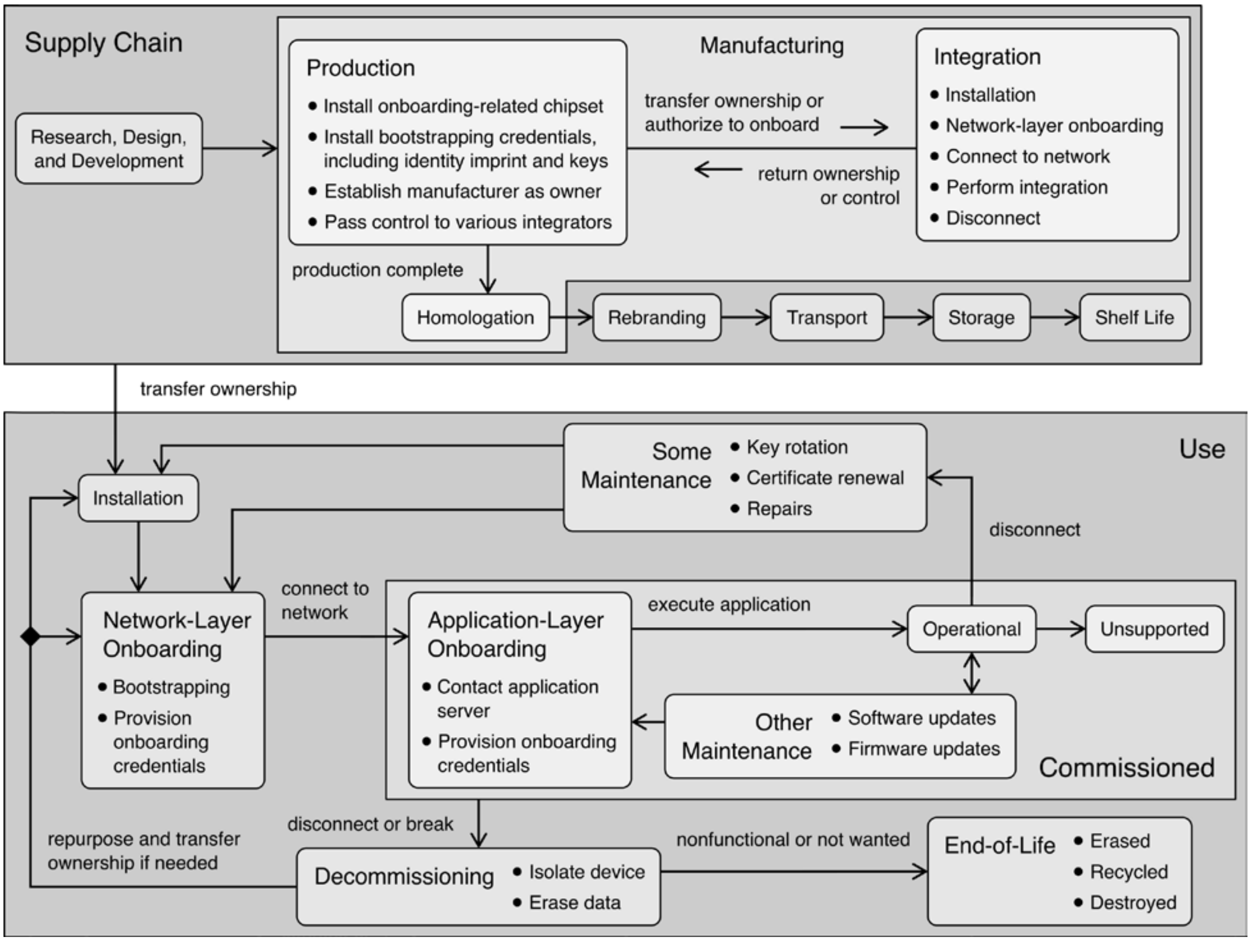

Figure 4-4 Complete IoT device life cycle from an onboarding perspective

5 Functional Roles

To accomplish onboarding, various proposed personnel roles are described. These roles may be filled by the same or different people or entities depending on the use case. (In a home setting, for example, many of these roles would fall to the device owner.) Also, the persons or entities filling these roles may change as a device moves through its life cycle (e.g., its owner and its authorized onboarders may change). The various identified onboarding-related functional roles and responsibilities are as follows:

- The **device manufacturer** creates the device, installs the device's bootstrapping credentials, and is the first owner of the device. The device manufacturer knows the intent of the device but is not able to imprint anything on the device that is unique to the device's specific network deployment. This is because, at the time the device is being manufactured, the details of its local network deployment are not known. The device manufacturer is responsible for creating and signing the device information declaration that contains the certificates of the device's owner and its other authorized onboarders (if any). The manufacturer is also responsible for keeping this declaration updated as the device ownership changes, though in theory it could delegate this responsibility to a trusted third party.
- The **device system integrator** is responsible for integrating a subcomponent of the device onto the device during the manufacturing process. To perform this integration, control of the device passes temporarily from the manufacturer to the system integrator and back. While the device is in possession of the system integrator, it may be required to onboard to the system integrator's network. In onboarding solutions that support proof of ownership and that restrict devices to onboarding only to networks that are owned or authorized by the device owner, the manufacturer either transfers ownership of the device to the integrator or authorizes the integrator to onboard the device so that the system integrator can onboard the device to its network.
- The **device owner** is the only individual or entity authorized to:
    - onboard and use the IoT device
    - grant another individual or entity the authority to onboard and use the IoT device
    - transfer ownership of the IoT device to another individual or entity

  An IoT device may have only one owner at any given time. If an onboarding solution supports a proof-of-ownership mechanism (Section 6.4.17), the device owner will be recorded in the device information declaration. The device's owner may change at various stages in the device's life. Ownership may change starting as early as being passed among different integrator-owners in the device manufacturing phase. Later, ownership will change when the device is acquired by its first post-production owner, and then again if the device is resold on the secondary market after a period of operational use. If an onboarding solution supports a proof-of-ownership mechanism, it also requires a mechanism to securely transfer device ownership from one entity to another, which will involve the device's current owner updating the device information declaration with information regarding the device's new owner. The device owner is also the entity that has the authority to determine the device's installer, onboarder, manager, and users as well as the application's owner, installer, manager, and users.

- The **device authorized onboarder** is the individual or entity authorized to onboard a given device to its network. This authorization comes from the device's owner and may be revoked by the device's owner. The device authorized onboarder would not typically have the authority to designate any other entity as a device authorized onboarder; only the device owner would be able to do this. A device may have multiple authorized onboarders at any given time. If an authorized onboarder needs to delegate onboarding ability to another party, it could request that the device owner add that party to the device's list of authorized onboarders.
- The **device purchaser** is the individual or entity that pays for or, in some cases, leases the IoT device. The device purchaser designates what individual or entity will be granted ownership of the device by the manufacturer when the device is acquired. The device purchaser is not necessarily the same as the device owner, onboarder, manager, or user.
- The **device installer** is the individual or entity (e.g., the IT team) that places the device at its deployment location and may turn it on.
- The **device onboarder** is the individual or entity that performs device onboarding.
- The **device manager** is the individual or entity responsible for managing the device. The device manager connects the device to the network, performs device software and firmware updates, and oversees all other device repairs and maintenance. When it is time for the device to be decommissioned, the device manager is the individual or entity that disconnects and isolates the device and erases all sensitive data, possibly performing a factory reset. When the device reaches end-of-life, the device manager removes all data from and destroys the device, possibly selecting certain parts for recycling. When the device is to be repurposed, the device manager transfers control of the device to its new authorized onboarder or new owner (as directed by the device's current owner).
- The **device user** is the individual or entity that uses the IoT device. From the viewpoint of the device and the network, the user is represented by his or her credentials.
- The **network owner** is the individual or entity that owns the network on which the IoT device is deployed. In the consumer use case, the network owner may be the same as the device user (i.e., the consumer), but in the enterprise use case, the network owner is typically a company. In some deployments, the device owner may be different from the network owner. For example, in a connected grid deployment, the connected grid of IoT sensors and other devices may be owned by one company, but the actual network on which the connected grid is running may be owned by a different organization. In onboarding solutions that support proof-of-ownership verification and mechanisms to grant authorization to onboard, where the device owner is not the same as the network owner, the network owner needs to be an authorized onboarder of the device.
- The **network administrator** is the individual or entity that manages the network and updates, maintains, and monitors networking-specific components (but not necessarily those of the network's IoT devices). The network administrator expresses its wishes through policy and enforces them via mechanisms such as the authorization service.

- The **application owner** is the individual or entity authorized to install, manage, and use a specific application on the IoT device. The application owner can grant others the authority to install, manage, and use the application. The application owner may be different from the network owner and from the device owner. For example, a consumer might have a solar panel set up on his or her home's roof. The solar panel is an IoT device that may be owned by either the consumer or the solar energy company. The solar panel is running a solar-energy-related application. The solar energy company owns the application, but the consumer owns the Wi-Fi network over which the solar energy application will send data back and forth to the cloud.
- The **application installer** is the individual or entity (e.g., the operational technology team) that onboards and installs the application to the IoT device. In some IoT devices, application installation may occur automatically during the application-layer onboarding process, based on the application-layer bootstrapping credentials that were included as part of the device's onboarding credentials.
- The **application manager** is the individual or entity responsible for managing the application. The application manager oversees application onboarding, initiates execution of the device's application, and helps manage the application by overseeing periodic application software updates. In addition, when the device is decommissioned, the application manager ensures that all application-specific sensitive data such as passwords, keys, logs, and user data that has been collected is erased.
- The **application user** is the individual or entity that uses the application on the IoT device to cause the device to perform its intended function. From the viewpoint of the application, the user is represented by his or her credentials.
- The **service provider** is the entity that operates the network that traffic transits to be sent to and from the internet from the IoT device's local network.

Throughout the device lifecycle, trust needs to be established and maintained between the device and the entities playing these various roles. For example, a medical device might need to trust a network owned by one entity but also connect to and trust cloud servers owned by another entity. Also, as the device moves through its life cycle, some of the above human roles move in and out of relevance to the device.

6 Onboarding Solution Characteristics

Numerous characteristics pertain to any potential onboarding solution. Onboarding solutions may vary from each other with respect to many attributes, including the level of security they provide, cost, and expertise required to operate the solution. As shown in Figure 6-1, for purposes of analysis, we have broken down these characteristics into four groups of characteristics that are predominantly:

- of interest to the individuals and enterprises that will deploy and use these onboarding solutions on their networks
- of interest to the companies that will manufacture and sell equipment that implements the onboarding solution—either network infrastructure components required to support the onboarding solution or IoT devices that implement the onboarding solution
- of interest to service providers (internet service providers [ISPs]/cable operators or application platform providers) that, depending on their business model, may take on a role to support trusted onboarding for IoT devices that their customers want to connect to their local networks
- security-specific (not depicted in Figure 6-1), which, when taken together, determine the overall level of security assurance that the solution will provide. Security characteristics are assumed to be of primary importance to all three groups listed above (users, manufacturers, and service providers). For discussion purposes, instead of duplicating the list of security characteristics in each of the above three groups, security characteristics are placed in a group by themselves and discussed separately.

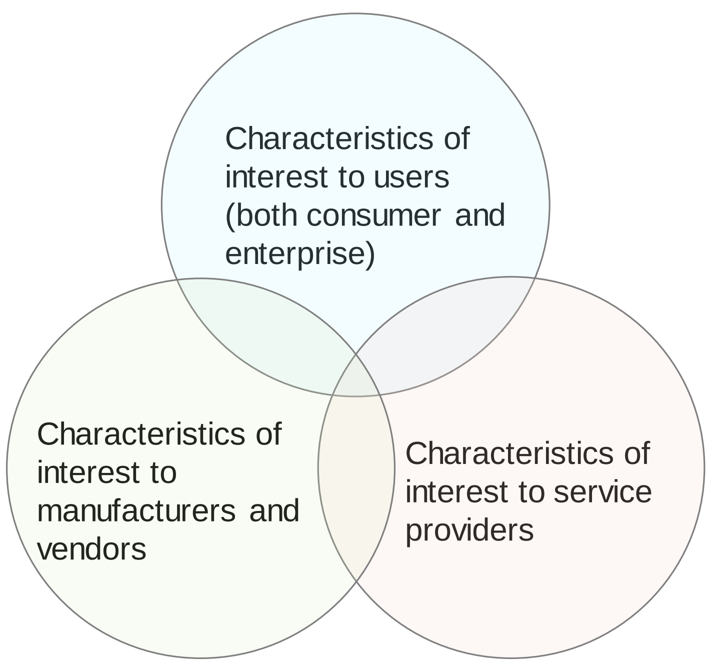

Figure 6-1 Types of onboarding solution characteristics

These four types of characteristics are listed and defined in tables in the next four subsections. Each of the security characteristics is also discussed in subsections of their own. These four types of characteristics are intended to serve as a taxonomy for describing and comparing onboarding solutions.

6.1 Characteristics of interest to users

Table 6-1 enumerates and defines onboarding solution characteristics that mainly interest IoT device users.

Table 6-1 Onboarding Solution Characteristics that Mainly Interest Users

Characteristic	Definition
ease of use	how easy the onboarding solution is to use (e.g., whether it works easily out of the box with little or no configuration or other effort; whether it requires the operator to have specific technical or security training or experience). For the consumer network environment, the ease-of-use characteristic is crucial. Solutions that require more technical or security knowledge than could reasonably be expected of a typical home network owner should not be considered for the consumer network environment.
network access technology	the potential network access technologies that the onboarding solution supports (e.g., whether it works on Wi-Fi, wired, or 5G networks only, or on some combination of these)
infrastructure dependencies	the infrastructure components required, either on the local network or in the cloud, to support the onboarding solution (e.g., AAA server, authorization service network onboarding component)
ease of integration into existing environment	the extent to which the current network infrastructure components, technologies, and mechanisms must change for the onboarding solution to be integrated into the network. For the consumer environment, it is crucial that the onboarding solution be able to be introduced to the current network with a very low level of friction.
number of new components introduced	the number of new systems, services, devices, or other elements that will be introduced to the current networking environment to support the onboarding solution
cost of required network infrastructure	the cost of the infrastructure that will be required to support the solution on the current network
cost of IoT devices	the additional cost that the onboarding solution will add to the cost of IoT devices that are manufactured to use it
discovery-initiated onboarding	the capability of the onboarding solution to automatically onboard a device after it has been discovered by the network infrastructure
hands-free (zero-touch)	the ability to onboard a device without manual intervention
bulk onboarding	the ability of the onboarding solution to support onboarding many devices in a very short period. Support for bulk onboarding requires that the solution be able to onboard devices hands-free (zero-touch) and that any virtual resources (e.g., local device identities and credentials) that may be needed to support onboarding be able to be secured and managed automatically and quickly.
onboard without internet access	the ability to onboard devices if the internet is not currently accessible. (An onboarding solution that requires access to a device information declaration that is not available on the local network would not, for example, have the characteristic of being able to onboard without internet access.)

Characteristic	Definition
provision of application data	the ability of the onboarding solution to automatically execute application-layer onboarding after network-layer onboarding has completed and the device has connected to the network. Such support could be provided, for example, by an onboarding solution that is designed to convey application-layer configuration information to the device as part of its onboarding credentials. Such information could, in theory, configure the device to consult a specific controller or application server, provide it with the credentials to authenticate to that controller or server, and initiate loading an application on the device.
device accessibility requirements	whether the onboarding solution requires the device to be accessible at certain periods of time and, if so, when. For example, the onboarding solution may require access to the device for operations such as security upgrades, key rotations, or certificate renewals. However, some use cases may require devices to be installed deep below the earth or in other difficult-to-access locations, which could limit their accessibility. It is important to ensure that the onboarding solution will not require access to the device when the device is inaccessible. Also, there may be regulatory requirements that prohibit the device from being accessed during certain periods; it is important to be aware of the onboarding solution's accessibility requirements to ensure that they are compatible with any regulatory requirements that may be imposed on the device by the onboarding solution.
deployment challenges	any drawbacks, deficiencies, or other characteristics (if any) that have not been listed already and that detract from the appeal of this solution or otherwise make it challenging to deploy
standards-based or proprietary	whether the onboarding solution is based on a standard or specification developed by consensus in an open forum and openly available or if it is proprietary. If it is proprietary, is the owner willing to bring the solution into an open forum where it would be open to modification and turned into an open standard? Are there any plans to do so? Users may be wary of adopting a proprietary onboarding solution for fear of getting locked into a proprietary ecosystem that could potentially limit their choices and increase their costs.
regulatory compliance	whether the onboarding solution meets regulatory requirements for any industry sectors, and which ones. Many industry sectors have their own specific regulatory requirements. Users are interested in whether the onboarding solution is compliant with regulations imposed on their own industry sector. For users in industry sectors subject to regulation, compliance of the onboarding solution with mandatory regulatory requirements is crucial; compliance with optional regulatory requirements may be desirable.
certification program	whether there is a certification program for validating if products (network equipment and IoT devices) correctly implement the onboarding solution. Such a certification program should be administered by an independent third party. Products can be certified as part of a larger system.
sustainability	the extent to which typical manufacturing, support, maintenance, and operation of the onboarding solution can be performed in a way that minimizes depletion of natural resources required to support these processes
security characteristics	the onboarding solution's security characteristics. A large collection of characteristics pertains to onboarding security. How trusted any given onboarding solution is depends on which of these security characteristics it has. These characteristics are enumerated in Table 6-4, and each is discussed more fully in the subsections of Section 6.4.

6.2 Characteristics of Interest to Manufacturers and Vendors

Table 6-2 enumerates and defines onboarding solution characteristics that mainly interest the companies that will manufacture and sell equipment that implements the onboarding solution—either network infrastructure components required to support the solution or IoT devices that implement the solution.

1244 **Table 6-2 Onboarding Solution Characteristics that Mainly Interest Manufacturers and Vendors**

Characteristic	Description and discussion of characteristic
specification status/maturity	how complete and well-vetted the written specification that documents the onboarding solution is. For example, are any aspects of the solution still waiting to be defined?
standards-based or proprietary	whether the onboarding solution is based on a standard or specification developed by consensus in an open forum and openly available or if it is proprietary. If it is proprietary, is the owner willing to bring the solution into an open forum where it would be open to modification and turned into an open standard? Are there any plans to do so? Manufacturers may be wary of adopting a proprietary onboarding solution, the specification of which is not under their control.
standardizing/owning body	the standardization body that controls the onboarding solution's specification, assuming the solution is standards-based. If the solution is proprietary, it refers to the vendor that owns it. For proprietary solutions, manufacturers are interested in whether the solution requires a license and, if so, how much it will cost.
implementation status/maturity	whether the onboarding solution has been implemented and, if so, how mature those implementations are. For example, are the implementations proof-of-concept prototypes or commercially available, production-grade products? Also, are any implementations open-source? How many different implementations of the solution are there? Have they been shown to be interoperable? Are network infrastructure components or chipsets available that support the solution? Are there IoT devices that support the solution?
solution implementers	what vendors, if any, make products that use or support the onboarding solution
regulatory compliance	whether the onboarding solution meets regulatory requirements for any industry sectors and, which ones. Many industry sectors have their own specific regulatory requirements. Manufacturers (in their role as users) are interested in whether the onboarding solution is compliant with regulations imposed on their own industry sector. In their role as vendors, they are also interested in whether the onboarding solution is compliant with regulations imposed on the industry sectors of their customers. They are also interested in understanding the extent to which compliance is mandatory or may just be desirable in terms of improving the onboarding solution's value. For industry sectors subject to regulation, compliance of the onboarding solution with mandatory regulatory requirements is crucial.
certification program	whether there is a certification program for validating if products (network equipment and IoT devices) correctly implement the onboarding solution. Such a certification program should be administered by an independent third party. Products can be certified as part of a larger system.
cost	the cost of goods and services required to produce and support products that implement the onboarding solution
manufacturing complexity	the degree of effort required of the IoT device manufacturer to support the onboarding solution. For example, how much effort is required for the manufacturer to create the device and provision it with its bootstrapping credentials? Does the manufacturer integrate the device with supply-chain security tools? How much effort is required of the manufacturer to support the device's onboarding, if any, after the device is sold (e.g., by maintaining a device information declaration that tracks device characteristics such as ownership)?
sustainability	the extent to which typical manufacturing, support, maintenance, and operation of the onboarding solution can be performed in a way that minimizes depletion of natural resources required to support these processes

Characteristic	Description and discussion of characteristic
IoT device requirements	the capabilities that the onboarding solution requires of IoT devices. A range of capabilities can be required of IoT devices, depending on the onboarding solution. These capabilities often correlate with device cost. Manufacturers need to understand the minimum capabilities that an IoT device requires to work with the onboarding solution. The following are some examples of potential device requirements: • equipped with a Trusted Platform Module (TPM) and the ability to perform certificate-based operations (i.e., random number generator, asymmetric cryptography) • equipped with a secure element to store device bootstrapping credentials • enough battery power to support encryption and other processing required for onboarding and still have sufficient power remaining to enable the device to last its expected lifetime • support for hardware-based encryption • support for digital signatures • support for eFUSEs to lock down firmware features and create immutable IDs • minimum memory requirements • support for Wi-Fi, wired, or 5G access technologies • amount of space required on chip for onboarding-related hardware and firmware and storage
device bootstrapping credentials	the device-specific information that the manufacturer is required to install on the device (e.g., identifier, keys, secrets, read-only field, X.509 certificate) for bootstrapping purposes. Is this information that a manufacturer can generate on its own in isolation, or is coordination with an external certificate authority required?
key type installed	the type of bootstrapping keys that the manufacturer installs on the device. Is a public/private key pair, a symmetric key, or both required?
security characteristics	the onboarding solution's security characteristics. A large collection of characteristics pertains to onboarding security. How trusted any given onboarding solution is depends on which of these security characteristics it has. These characteristics are enumerated in Table 6-4, and each is discussed more fully in the subsections of Section 6.4.

6.3 Characteristics of Interest to Service Providers

Depending on the business model, service providers (e.g., ISPs/cable operators or application platform providers) may choose to play a role in supporting device onboarding. However, onboarding support by service providers is not required.

If the steps performed to support trusted onboarding are difficult, it is likely that some consumers will not bother to perform them. Even those consumers who are diligent about trying to perform the steps may not be able to do so correctly, with the result that onboarding may not be performed securely. To address this problem, depending on the business model, the consumer's ISP or cable operator may choose to assist with onboarding and, in doing so, increase the security of the consumer's network while also providing the consumer with a better overall experience. For example, most consumer networks can benefit greatly from an environment in which each device has its own identity and its own credentials, characteristics that are typically associated with enterprise-level security. However, the consumer does not necessarily have the technical skills or the desire to set up and maintain an AAA server, an authorization service, or any similar infrastructure that would be required to support access control enforcement based on device identities and credentials. Consumers would love to have enterprise-level security capabilities in the consumer space without any of the headache or overhead of supporting these capabilities. If service providers take a role in supporting secure onboarding for their customers, such enterprise-level security may be possible without requiring much extra work, if any, on the part of the consumer. Depending on the business model, service providers could operate and manage authorization and other services and infrastructure in the cloud on behalf of consumers. Table 6-3 enumerates and defines onboarding solution characteristics that mainly interest service providers (e.g., ISPs/cable operators and application platform providers).

Table 6-3 Onboarding Solution Characteristics that Mainly Interest Service Providers and Operators

Characteristic	Description and discussion of characteristic
specification status/maturity	how comprehensive and well-vetted the written specification that documents the onboarding solution is. For example, are any aspects of the solution still waiting to be defined?
standards-based or proprietary	whether the onboarding solution is based on a standard or specification developed by consensus in an open forum and openly available or if it is proprietary. If it is proprietary, is the owner willing to bring the solution into an open forum where it would be open to modification and turned into an open standard? Are there any plans to do so? Manufacturers may be wary of adopting a proprietary onboarding solution, the specification of which is not under their control.
standardizing/owning body	the standardization body that controls the onboarding solution's specification, assuming the solution is standards-based. If the solution is proprietary, it refers to the vendor that owns it. For proprietary solutions, manufacturers are interested in whether the solution requires a license and, if so, how much it will cost.
implementation status/maturity	whether the onboarding solution has been implemented and, if so, how mature those implementations are. For example, are the implementations proof-of-concept prototypes or commercially available, production-grade products? Also, are any implementations open-source? How many different implementations of the solution are there? Have they been shown to be interoperable? Are network infrastructure components or chipsets available that support the solution? Are there IoT devices that support the solution?
solution implementers	which vendors, if any, make products that use or support the onboarding solution
regulatory compliance	whether the onboarding solution meets regulatory requirements for any industry sectors and, which ones. Many industry sectors have their own specific regulatory requirements. Service providers (in their role as users) are interested in whether the onboarding solution is compliant with regulations imposed on their own industry sector. In their role as service providers, they are also interested in whether the onboarding solution is compliant with regulations imposed on the industry sectors of their customers. They are also interested in understanding the extent to which compliance is mandatory or may just be desirable in terms of improving the onboarding solution's value. For industry sectors subject to regulation, compliance of the onboarding solution with mandatory regulatory requirements is crucial.
certification program	whether there is a certification program for validating if products (network equipment and IoT devices) correctly implement the onboarding solution. Such a certification program should be administered by an independent third party. Products can be certified as part of a larger system.
cost	the cost of components and resources required to deploy and provide operational support for the onboarding solution
operational complexity	the degree of effort that is required of the service provider to provide operational support for the onboarding solution. How much effort is required to perform the initial deployment as well as ongoing day-to-day operation of the onboarding solution.

Characteristic	Description and discussion of characteristic
sustainability	the extent to which typical manufacturing, support, maintenance, and operation of the onboarding solution can be performed in a way that minimizes depletion of natural resources required to support these processes
additional features to improve benefits	whether there are additional features, beyond secure onboarding, that the service provider might be able to provide to the consumer, by virtue of the service provider's support for onboarding, that might further improve the consumer's experience
security characteristics	the onboarding solution's security characteristics. A large collection of characteristics pertains to onboarding security. How trusted any given onboarding solution is depends on which of these security characteristics it has. These characteristics are enumerated in Table 6-4, and each is discussed more fully in the subsections of Section 6.4. If an onboarding solution requires service provider support, the service provider's reputation may be impacted by the level of security that the onboarding solution provides.

6.4 Security-Specific Characteristics

A key characteristic of any onboarding solution is the overall level of security assurance that it provides. This level of assurance is determined by the solution's security-related attributes and capabilities. These security-related attributes and capabilities are enumerated and defined briefly in Table 6-4. They are also discussed further in the subsections that follow Table 6-4. It should be noted that some of these attributes are more objective than others. For example, attributes such as device identification are concrete; either the onboarding solution leverages device identification, or it does not. Other attributes, such as supply-chain security, are more subjective. They are contextual and vary on an organization-by-organization basis: an onboarding solution may be able to integrate with the supply-chain management tool of one organization but not with that of another. We include both objective and contextual characteristics, under the reasoning that both types would be included in an organization's checklist when determining whether a given onboarding solution meets the organization's requirements.

Table 6-4 Security-Specific Attributes and Capabilities of an Onboarding Solution

Attribute/Capability	Description
security model	whether the mechanism that parties use to gain each other's trust is based on signed vouchers or proof of knowledge
device identity	information used to identify the device and distinguish it from other devices
device authentication	verification that the asserted identity of a device is the device's actual identity
device authorization	determination of whether a device should be permitted to connect to the network
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.
maintainable credentials	credentials that expire, can be revoked, and can be renewed relatively easily
device type verification	verification that the device is of the asserted type or from the asserted manufacturer (as opposed to verifying that it has a specific identity)
device attestation	proof that some elements of the device (e.g., firmware) have not been tampered with

Attribute/Capability	Description
trust anchors/root of trust	elements that security depends on; if they are compromised, security is undermined
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?
key type	type of keys used (e.g., symmetric, pre-shared, public/private)
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
network selection	determination by the device regarding what network it should join
network authentication	verification that the asserted identity of a network is the network's actual identity
network authorization	determination of whether a network should be permitted to onboard (i.e., take control of) a device
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
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.
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.
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.
privacy	ability of the onboarding solution to prevent unauthorized disclosure of personal information during and related to the onboarding process
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.

Attribute/Capability	Description
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.
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.

Each of the security characteristics in Table 6-4 is discussed more fully in the following subsections.

6.4.1 Security model

The onboarding solution's security model refers to the type of mechanism that parties use to gain each other's trust at the start of the onboarding process. This mechanism may be based on vouchers (i.e., information signed by a trusted third party) or proof of knowledge. Proof of knowledge is a mechanism whereby one party proves to another that it possesses a certain secret (e.g., a pre-shared key).

Parties that may have to gain each other's trust as part of the onboarding process could include:

- IoT devices attempting to gain the trust of the network onboarding component
- network attempting to gain the trust of an IoT device that it wants to onboard
    - may involve the network owner attempting to gain the trust of the IoT device

6.4.2 Device identity

A device's identity is any information that is used to identify the device and distinguish it from other devices. Device identities that are irrevocable and immutable—those that are not easily spoofed, modified, or copied from memory—are most secure, and identities that can be cryptographically verified are strongest. Some examples of strong identities are:

- DevID [15], which is:
    - stored and manipulated in the device TPM or secure element, so it is not easily modified or copied from memory
    - an X.509 certificate, so it can be used to cryptographically verify device identity, making it difficult to spoof a device or modify an identity

  - installed during manufacturing (as opposed to LDevIDs, which are installed locally and can serve as locally significant device IDs)
  - reliant on the public key infrastructure and the certificate authority that issued the X.509 cert to provide a chain of trust
- DICE CDI (Trusted Computing Group) [16], which:
  - serves as a device identity and as an attestation of device firmware, thereby providing some proof that the IoT device firmware has not been tampered with
  - is derived from a unique device secret and the identity of the device's first mutable code, so it is not easily modified or spoofed
  - does not require a TPM, so it does not increase silicon requirements as much as a DevID
  - is implemented in hardware during manufacturing
- International Organization for Standardization (ISO)/International Electrotechnical Commission 20008 standardized direct anonymous attestation (DAA), which
  - provides an irrevocable identity that is immutably written into processors that implement DAA
  - preserves privacy because it does not use X.509 certificates, which are public and visible in clear text
  - Intel Enhanced Privacy ID is an implementation of ISO 20008 that provides direct anonymous attestation, which provides the ability to authenticate a device for a given level of access while allowing the device to remain anonymous and to have that device's individual authority revoked if its private key has been compromised [17].
- 5G certificate-based embedded subscriber identity module (eSIM)
  - eSIM (an embedded Universal Integrated Circuit Card) that may be soldered inside a mobile device that can accommodate multiple SIM profiles for use with different operators so the device can be connected with whatever operator's network the end user selects [18]
- Devices designed to onboard using the Device Provisioning Protocol (DPP)
  - DPP-capable devices are not necessarily imprinted with an explicit identity. Initially, they can be identified uniquely by the value of the private bootstrapping key they have stored securely on them. This value is not revealed or explicitly used as an identity, but it is cryptographically bound to the device through public key cryptography. This private key is not necessarily signed, but it is intended to be unique to the device. Later, as part of the DPP onboarding process, a device is provisioned with unique credential information in the form of a connector, which includes a network access key that is unique to the device. This connector may be considered an implicit identity for the device while it is on the network. The DPP configurator signs the connector before provisioning it to the device, and the device uses the connector to establish security associations with other onboarded devices.

While DevIDs are the most secure, that security comes at a cost because it relies on the existence of a robust and secure X.509 certification infrastructure as well as on devices themselves being equipped with TPMs or secure elements.

Read-only fields such as device serial numbers and International Mobile Equipment Identities that are used to identify mobile phones can also be used as device identities and are much less costly to implement and support. However, they are less secure than other mechanisms because they are not cryptographically bound to the device. This makes them susceptible to being spoofed or modified. These weak identifiers may not be considered secure enough to support some use cases.

As a device moves through the various roles of its life cycle, the users that are interacting with it may find it useful to assign the device additional identities. For example, a device will have a network-layer identity based on its IP address once it has been connected to the network, but its manager or someone else interacting with it may also assign the device a human-readable identity that makes it easier for him or her to keep track of the device. The device's application manager might also assign the device an application-layer identity. For purposes of onboarding, however, the identities that are relevant are:

- the device's original identity, which is included in the device's bootstrapping credentials and which the network onboarding component uses to authenticate the device (assuming the onboarding solution supports device authentication)
- a second identity that may be assigned to the device as part of its onboarding credentials, which is significant only on the local network (e.g., a LDevID or other X.509 certificate may be issued to the device as an onboarding credential that the device needs to authenticate itself to the local network)

6.4.3 Device authentication

Device authentication (i.e., verification that the asserted identity of a device is the device's actual identity) is closely tied to device identity. To be strongly authenticated, the device asserts a specific identity, and that identity is cryptographically bound to the device. In some onboarding situations, a device may not be asserting a specific identity; instead, it may simply be asserting to be a particular type of device or to be from a particular manufacturer. In such cases, it is not possible to authenticate the device, though it may be possible to verify device type (see Section 6.4.7).

For the device to be authenticated cryptographically, it needs to have credentials installed on it. For example, in the case of a device that uses a DICE CDI as its identifier, the DICE CDI has to be implemented in hardware during manufacturing, and it requires the manufacturer to provide a unique device secret. A device that uses a DevID as its identifier requires an X.509 certificate and the private key that corresponds with the public key in that certificate installed during manufacturing. When either type of device is onboarded, the device's identity can be cryptographically authenticated. Once a device that uses a DevID has been authenticated in the initial part of the onboarding process, the network onboarding component will install a locally significant device identifier (an LDevID) on the device as part of the device's onboarding credentials. Provisioning an LDevID to the device involves installing a new X.509 certificate and corresponding private key on the device. There are several advantages to installing such a local certificate-based identifier on the device, including:

- The manufacturer will not be privy to the device's new private key, thereby eliminating one avenue of exposure to potential attack.
- Having local certificates for its devices provides the local network with better control over those devices because it can revoke the devices' certificates at any time, and it is more efficient and reliable to check a certificate revocation list (CRL) locally than to depend on the manufacturer's CRL for every transaction.

Cryptographic-based authentication usually relies on one or more trust anchors. These trust anchors may be preset within the device. In some cases, this trust may be established out of band. Authentication that is performed based on certificates requires the certificate's root certificate authority to be trusted. It also requires trust that the manufacturer or other entity that installed the private key on the device has not disclosed and will not disclose that information. It is important to understand the trust anchors and the chain of trust that flows from them, because security of the authentication process relies on them.

In some onboarding solutions, a device may assert a read-only field, such as a serial number or Media Access Control (MAC) address, as its identity. Even though this identity may be read from the device and verified to be as asserted, if this identity is not cryptographically bound to the device, the device authentication is considered weak because there is not strong assurance that the identity actually belongs to the device. In these cases, trust is placed in the person who is onboarding the device, because that person is being relied upon to ensure that the device he or she is onboarding is the device that he or she intends to onboard.

6.4.4 Device authorization

Device authorization refers to the process of determining whether a device should be granted access to the network. Device authorization typically occurs only after a device has been authenticated (i.e., after the device has been verified to have the identity that it claims to have). If a device fails authentication, it would not be authorized to use the network at all. If a device is successfully authenticated, determination regarding whether it is authorized to connect to the network (and, if so, what network resources it has permission to access) depends on network policy.

In an enterprise network, this policy is typically expressed in an AAA server or equivalent authentication, authorization, and accounting services that receive requests for access to the network and other resources and consult a database to determine what entities should be granted access to what resources. The authorization service has to be configured with the identity and access permissions of each device that will connect to the network before those devices will be permitted to connect to the network.

Consumer networks do not typically have local AAA servers or authorization services that can perform device authorization determinations. However, in theory, depending on its business model, a service provider could operate an authorization service on behalf of its customers to provide those customers with a device authorization service. Therefore, onboarding solutions designed to be supported by service providers could include device authorization among the onboarding solution characteristics supported.

Onboarding solutions used on consumer networks that do not have access to an authorization service do not typically support device authorization. For example, in many cases, if a device presents its network password to a consumer network access point, the device is by default granted access to all resources on the local network (unless the consumer network supports MUD and the device has an associated MUD file that prevents such access).

6.4.5 Secure local credentialing capability

Secure local credentialing capability refers to the ability of an onboarding solution (as distinct from a device manufacturer) to provision credentials to a device in a manner that protects them from disclosure both while in transit to the device and while stored on the device. The ability to perform secure local credentialing should be considered a mandatory capability of every onboarding solution. Securely provisioning local credentials to the device is, in fact, the goal of the onboarding process. Such local credentials are defined as onboarding credentials in Section 2.2, and they are significant with respect to the local network. They are provisioned to the device during onboarding and remain on the device in addition to the bootstrapping credentials that were provisioned on the device before the device was onboarded. These credentials include all the information that the device needs to connect to the local network. They can include locally significant device identifiers, certificates, keys, an identifier for the network to which the device should connect, and other credentials that enable the device to gain access to local resources and applications. Because they are installed by the network onboarding component of the local network, these credentials are not known to the manufacturer, and the owner is in complete control of their expiration and revocation.

Ideally, the onboarding process does not require those credentials to be disclosed to any humans, and it can provision unique network credentials to each device. They are provisioned during onboarding, but they can later be updated, replaced, and, ultimately, deprovisioned, thereby restoring the device to its pre-onboarding state in which only its original bootstrapping credentials are installed.

6.4.6 Maintainable credentials

The onboarding credentials that are provisioned to the device during onboarding are needed for the device to connect to the network. Some credentials, such as shared secrets, may be relatively simple insofar as they are unable to expire. Other credentials, such as X.509 certificates and JSON web tokens, are more sophisticated. They may have attributes that can be manipulated to provide control over their validity. For example, these credentials may be able to expire, be revoked, or be renewed. We refer to these latter types of credentials as maintainable credentials. If an onboarding solution uses maintainable credentials and the solution includes mechanisms that can be performed relatively easily to ensure that the credentials provisioned to devices can be renewed or revoked, the onboarding solution is considered to support maintainable credentials. To ensure that a device's credentials are maintainable, the onboarding solution could be designed so that it is possible for an authorized entity to delete the device's onboarding credentials. Deleting a device's onboarding credentials and then re-onboarding the device is one way of replacing the device's existing credentials with new ones, if necessary.

6.4.7 Device type verification

Device type verification refers to the ability to verify that a device is of the asserted type or from the asserted manufacturer. It should not be confused with device authentication, which is the ability to verify that the asserted identity of a device is the device's actual identity. A device's identity is specific to that device, but a device's type is an attribute that the device shares with other devices of the same manufacturer and model. If a device's identity has been authenticated, then, by definition, the device's type has also been verified. On the other hand, a device may have its type verified without having its identity authenticated.

In some onboarding situations, a device may not claim to have a specific identity; it may simply assert to be of a particular make and model. For example, a network may need to ensure that the device it is onboarding is a certain type of light bulb, but it may not matter what specific light bulb it is. In this latter case, the onboarding solution would, at a minimum, need to support device type verification.

6.4.8 Device attestation

In some use cases, a network may be so critical that authenticating a device may not be sufficient for determining whether the device should be allowed to onboard to the network. The network may also require some form of device attestation, i.e., proof that the device has not been tampered with. Device attestation refers to the ability to provide proof that elements of the device (e.g., firmware) have not been tampered with. DICE integrated development environments (IDEs), which were discussed in Section 6.4.2, are examples of mechanisms that can be used in an onboarding solution to support device attestation. DICE IDEs serve not only as device identities but also as attestations of device firmware. Onboarding solutions that use DICE IDEs thereby provide some proof that the device firmware has not been tampered with.

Some IoT devices, when booted, will verify the onboard chip certificate and then, in stages, verify the authenticity and integrity of all the firmware images that will be executed. This secure boot process can also verify device application integrity by calculating the application hash and comparing it to a known value to ensure that the application has not been unexpectedly modified; it can also verify authenticity of the software on the device by using a digital signature (or a hash of the digital signature in resource-constrained applications).

Devices that support attestation can generate signed attestation tokens that make claims about the device (e.g., ID, manufacturer, model, installed software, versions, boot state, measurements, and integrity checks of running firmware and software). This attestation token is sent to the network and evaluated to verify the authenticity and integrity of the device and to decide whether it is sufficiently trustworthy that the network should permit the device to be onboarded. 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 a private key known only to the device. The secure boot process can build on that root of trust 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 [19].

6.4.9 Trust anchors/root of trust

The security of any onboarding solution is ultimately based on trust. It is important to understand what elements of the solution are trusting what other elements of the solution and how the trust is established. An onboarding solution's root of trust (i.e., its trust anchors) is those elements on which security depends. These are the elements that are assumed to be trusted so that, if they are compromised, security is undermined. The root of trust is arguably the most crucial element with respect to determining how trusted the onboarding solution is.

In some onboarding solutions, the root of trust may lie with a person, such as the individual who performs the onboarding. This person is trusted to ensure that the device being onboarded is the correct device, that the network to which it is being onboarded is the intended network, and that the device is authorized to be onboarded to that network. The trust anchor lies with the person because he or she is assumed to have the authority and/or physical control over the device to onboard that device to the network in question. Authorizing an untrustworthy person to perform onboarding for a network, therefore, would undermine that network's operational security.

In some use cases, a requirement to trust the individual who is performing the onboarding may not be sufficiently secure. In these use cases, a root of trust may be required to reside within the device itself. The most secure onboarding solutions are rooted in a hardware root of trust. A hardware root of trust refers to hardware security features that isolate, protect, and securely store identities, security keys, and other essential data that the onboarding solution relies upon for secure operation. A device whose identity and credentials are based in the device hardware (e.g., DevID, DICE CDI) so that they cannot be modified easily has a hardware root of trust. As mentioned in Section 6.4.8, an IoT device can be designed to perform a secure boot process to establish a root of trust. The boot process could include steps to, for example, verify the device's chip certificate, the authenticity and integrity of its firmware, the integrity of its application, and the authenticity of its software.

Hardware roots of trust require trust that the hardware itself was built correctly and that the appropriate certificate was installed on it. The hardware-based root of trust is only as reliable as its manufacturer. In some cases, IoT devices may be built in environments that have lax security.

In other cases, IoT devices may be built in well-controlled security environments but, with some manufacturing processes being performed outside the United States, may be more vulnerable to supply-chain attack. In these situations, a certificate that has been installed in the hardware may not be an appropriate mechanism on which to rely when performing device authentication. In fact, it may be worse for security by providing a false sense of assurance. The reality is that when certificates are being installed during the manufacturing process and the supply chain is vulnerable or compromised, this invalidates the onboarding solution's root of trust and undermines operational security.

There are additional trust anchors on which an onboarding solution may rest. For example, in an onboarding solution that supports proof-of-ownership verification, the entity that signs the device information declaration is one of the trust anchors. Similarly, if a device has a MUD file, the mechanism that associates that MUD file with the device may need to be trusted, the manufacturer of the device needs to be trusted to have accurately described the device's communications requirements in the MUD file, and the signer of the MUD file needs to be trusted.

Regardless of an onboarding solution's trust anchors, it is important that they be explicit and well understood, because the solution's security depends on them not being compromised.

6.4.10 Trusted onboarder required

The trusted onboarder required characteristic refers to whether the onboarding solution requires the person who initiates or performs the device onboarding process to be trusted. The trusted onboarder required characteristic is closely related to the trust anchors/root of trust characteristic. An onboarding solution requires a trusted onboarder if the person onboarding the device must be trusted to ensure that the device being onboarded is the correct device, that the network to which it is being onboarded is the intended network, that the device is authorized to be onboarded to that network, or that the network is authorized to have the device connect to it. If these authentication and authorization operations can be performed regardless of who is performing the onboarding, perhaps by automatic network and device authentication based on presented credentials and information in the device information declaration, then a trusted onboarder is not required.

It should be noted that even if a trusted onboarder is required, under no circumstances should the onboarding solution require or even permit the trusted onboarder (or any other individual) to have access to the credentials that are being onboarded to the device. Onboarding, as we have defined it in Section 2.1, is the process of provisioning a device's onboarding credentials over a secure channel that has been established between the device and the network onboarding component. By definition, onboarding does not provide an opportunity for the device's network credentials to be revealed to the trusted onboarder (or any other individual), thereby eliminating the insider threat that would arise from revealing these credentials to the onboarder.

6.4.11 Key type

Onboarding solutions may require and make possible the use of various types of keys at various points in the onboarding process. The device to be onboarded is already provisioned with a bootstrapping key prior to the onboarding process, as a mechanism to establish trust between the device and the network onboarding component at the start of the onboarding process. This key could be a private key that is part of a public/private key pair, or it could be a pre-shared key. Using a pre-shared key (i.e., a key that is known prior to the bootstrapping process to both the device being onboarded and the network onboarding component) is subject to the risk of that key having been disclosed at some point during the out-of-band process by which it was conveyed to both entities. Using private keys that are part of public/private key pairs avoids this risk. Once trust is established between the device and the network onboarding component and they establish a secure channel between them, this secure channel provisions onboarding credentials to the device, including a credential that the device can use to connect to the network securely once onboarding is complete. The credential that will typically be provisioned to the device is a symmetric key that the device and the network will use as a session key to encrypt operational traffic that they exchange.

6.4.12 Encryption details

In addition to the type of keys used, other encryption-related details are also crucial in determining the level of security supported by the onboarding solution. These details include both attributes and characteristics that affect security in theory, such as the encryption standard used, key length, mode, and whether forward secrecy is supported; they also include attributes and characteristics that affect security in practice, such as cryptographic library version (i.e., has it been found to have any bugs).

6.4.13 Network selection

Network selection refers to the determination made by the device regarding what network it should join. There may be numerous different networks within range of the device when it is powered on, so the question arises as to how the device determines what network it should onboard. If an onboarding solution is to be truly automated, it has to support some mechanism for the device to determine what network it should join. For example, a network SSID could be provisioned to the device as part of its onboarding credentials. Alternatively, device ownership information derived from the device information declaration could be used to determine what nearby networks are operated by the device's owner or by an operator that has been designated as an authorized onboarder for the device (see Section 6.4.17 and Section 6.4.19). If such a network can be identified, the device will onboard to it. The ability for a device to select the correct network to which to onboard is a key capability for an onboarding solution.

6.4.14 Network authentication

Network authentication is verification that the asserted identity of a network is the network's actual identity. Not only is a device required to know which of multiple networks that are in range it should connect to, but, for the utmost security, the device should verify that the network to which it has determined to onboard (and which will therefore take control of it) is the network that it claims to be. This enables the owner of the IoT device being onboarded to have some assurance that the device is not connecting to a rogue access point that is masquerading as a legitimate network (e.g., by advertising the SSID of the legitimate network and using a stronger signal than that output by the legitimate network). Network authentication provides assurance to the device that it is connecting to a legitimate network.

To support network authentication, the network onboarding component would have to present the IoT device with credentials (e.g., an X.509 certificate) that are cryptographically bound to the network so that these credentials could not easily be used by rogue access points to masquerade as the legitimate network. In some onboarding solutions, network authentication may not be supported; the device makes no attempt to verify the legitimacy of the network's asserted identity. Instead, a trusted individual who is performing the onboarding is relied upon to determine that the network to which the device is being onboarded is the intended network. In all cases, whether the identity of the network is cryptographically authenticated or a trusted third party is relied upon to attest to the network's identity, it is important to understand upon what trust anchors the solution is relying.

6.4.15 Network authorization

Network authorization refers to the process of determining whether a network should be allowed to onboard (i.e., take control of) a device. Network authorization would typically be performed after network authentication has verified that the network has the identity it purports to have. Network authorization decisions could be based on information derived from the device information declaration that, for example, lists what networks are authorized to onboard a device, as discussed in Section 6.4.19.

6.4.16 Connected device and onboarded device cross-check

To ensure the security of any network, it is important to ensure that all devices connected to the network are authorized to be on the network. An onboarding solution that integrates with a network monitoring application may, together with that network monitoring application, provide an automated mechanism to continuously monitor the network to identify connected IoT devices and ensure that each of these devices was onboarded via the network's onboarding process, is authorized to be connected to the network, and is expected to be up and running. The ability to cross-reference the list of connected devices with the list of onboarded devices is a valuable tool in helping identify rogue devices that may have been provisioned with network credentials in an irregular or unauthorized process that is designed to circumvent established security policy and procedures.

6.4.17 Proof of ownership

Proof of ownership, in general, refers to the ability to determine what individual or entity owns each IoT device. Some IoT manufacturers may create and sign device information declarations (discussed in Section 2.7) or similar mechanism that securely tracks ownership of their IoT devices. With respect to onboarding, proof of ownership refers to whether the onboarding solution can integrate with the manufacturer's proof-of-ownership mechanism to support a secure, automated process for determining what individual or entity owns a device. In some current enterprise IoT deployments, the organization that has purchased an IoT device is required to claim the device before the organization is permitted to install the device. Making such claims is often a manual process, requiring information to be entered in a web-based application or a phone call to the device manufacturer. As such, it can be time-consuming, error prone, and frustrating.

As defined in Section 5, a device's owner is the individual or entity that is authorized to onboard, install, manage, and use an IoT device; the owner is also the individual or entity that is authorized to authorize others to onboard the device. A device's owner typically changes as the device moves through its life cycle. The owner may be an integrator who is currently authorized to operate and control the device as the device progresses through the manufacturing process, before it leaves its final factory floor; the party that initially acquired the device after it completed manufacturing (likely as a result of purchasing the device); or a party that acquired the used device from a previous owner when it was sold on a secondary market.

If a device manufacturer supports a proof-of-ownership mechanism, it is ideal if the onboarding solution can integrate with that mechanism so it can make ownership assurances regarding devices that are attempting to onboard. A proof-of-ownership mechanism could be used to determine whether the network to which a device is attempting to onboard (i.e., the network that is attempting to take control of the device) is owned by the same entity as the device owner. If so, this could provide assurance that the device was acquired to use it on this network and thereby indicate that such onboarding should be permitted. In addition, a proof-of-ownership mechanism could help protect a device from being intercepted and taken over by a rogue network that attempts to onboard the device at some point in the supply chain, before the device reaches its intended installation point.

Note that support for a proof-of-ownership mechanism would require the device manufacturer (or other entity supporting the mechanism) to create the device information declaration and keep it updated to securely track ownership information. This responsibility would continue well beyond the date that the device is initially sold and extend at least until the device reaches end-of-life.

6.4.18 Secure ownership transfer

Support for proof of ownership goes hand in hand with support for secure ownership transfer. As has been described, the owner of a given device may change multiple times during the device's life cycle. If a device manufacturer supports a proof-of-ownership mechanism, the manufacturer also needs to provide a secure ownership transfer mechanism along with it. These mechanisms are required to be used in tandem to ensure that proof-of-ownership assurances are accurate no matter how many different owners a device has passed through.

Specifically, mechanisms are needed that enable:

- the device's initial owner to be securely documented
- the device's current owner to securely transfer ownership to another individual or entity

It cannot be possible for a third party to acquire ownership of a device without the express permission of the device's current owner.

In the consumer space, a practical example of when secure ownership transfer is relevant is when a house is sold to a new owner, and IoT devices (e.g., sensors, light bulbs, cameras) convey with the house. A mechanism is required to ensure that only the new homeowner has the authority to install, manage, and use these devices (or to authorize others to do so). If the onboarding solution that the owner is using is integrated with the proof-of-ownership and secure ownership transfer mechanisms, then the onboarding solution could ensure that none of the IoT devices that conveyed with the house could connect to the homeowner's network unless and until their ownership is transferred to the current homeowner. While it is desirable for onboarding solutions to support secure ownership transfer, it should be recognized that the secure ownership transfer mechanism may introduce an attack vector.

6.4.19 Onboard only to authorized networks

An IoT device's owner is the individual or entity that is authorized to determine to what networks the device should be able to connect. In some cases, the device's owner may want to restrict that device to onboard only to networks belonging to the device owner. In other cases, the device owner may want to grant additional network owners the authority to onboard the device. If information is available regarding the networks that are authorized to onboard a device, this information can be consulted to ensure that the device is not being onboarded to an unauthorized network. This sort of information can be stored in the device information declaration described in Section 2.7. Such authorized onboarder information could be provided to the device prior to onboarding, so that the device can determine if the network is authorized to take control of it. For this mechanism to work, the information in the device information declaration regarding the device owner and the networks to which the device is permitted to onboard needs to be relied upon as accurate and up-to-date.

To ensure that device owners can grant networks other than their own the authority to onboard the device, mechanisms are needed that enable:

- the device's current owner to securely authorize additional entities to onboard the device
- the device's current owner to securely revoke authorization for other entities to onboard the device
- the current list of entities authorized to onboard the device to be securely documented

6.4.20 Privacy

Privacy in the context of onboarding refers to the ability of the onboarding solution to prevent unauthorized disclosure of personal information during and related to the onboarding process. Because onboarding occurs before the device connects to the network and is used operationally, the information that is conveyed between the device and the network onboarding component during the onboarding process would not be expected to explicitly include personal information. The information conveyed during onboarding typically includes device-specific information such as device identifier, device credentials, and MUD URL rather than any individual's personal information. However, information conveyed in the device information declaration could potentially include information identifying the device owner and entities that are authorized to onboard the device. If so, the confidentiality of this information has to be protected, both while it is in transit and after it is at rest, to minimize the possibility that it will be disclosed to unauthorized individuals; the integrity of this information should also be protected from unauthorized modification. It is also possible that even though the information conveyed during the onboarding process does not explicitly contain personal information, it may nevertheless implicitly reveal personal information. Just knowing that a device is of a specific type (e.g., a medical infusion pump) and knowing the network to which it is being onboarded may imply sufficient personal information about the device's user to be considered a breach of privacy.

During its operation, a device may have personal information stored on it. If the device is to be resold or repurposed, it is imperative that authorized users can delete this personal information before the device changes ownership. Depending on the onboarding use case, there may be specific privacy requirements that the onboarding solution is required to support. Whether a given onboarding solution can support those requirements will be a distinguishing factor in determining its suitability. At this point, the privacy-related characteristics of onboarding solutions are not completely understood. This is one area in which we hope to receive input from the broader community, including industries for which privacy is a primary concern.

6.4.21 MUD support

MUD support refers to whether the onboarding solution supports conveyance of a device-specific MUD URL to the network. If an onboarding solution provides MUD support, MUD can enforce the device's communications profile once the device is connected to the network. Ideally, the onboarding solution should provide a mechanism for strongly binding the MUD URL to the device, such as providing the MUD URL in the device's X.509 certificate. If the MUD URL is not strongly bound to the device and conveyed securely, it may be possible for the device to be associated with a fraudulent MUD file and thereby gain additional network access beyond that intended by its actual MUD file.

6.4.22 Evolving communications profile enforcement

As explained in Section 6.4.21, an onboarding solution that supports MUD enables the device's communications profile, as defined in the device's MUD file, to be enforced after the device has connected to the network. Evolving communications profile enforcement refers to the ability of the onboarding solution to enforce an evolving communications profile for the device—a profile that changes as the device moves through its lifecycle.

We typically define an IoT device as being single purpose, but when we do so, we have its ultimate application-level purpose in mind (i.e., the functionality that the device performs when it is connected to the network and its application is executing). However, before and after a device gets to this phase of its life, it may have a succession of other, smaller purposes that serve to achieve its single application-level purpose. As an IoT device moves through its life cycle, it takes on various roles that change according to the life phase. When it is initially acquired, its purpose is to be onboarded at the network layer. Once it has completed network-layer onboarding, its purpose is to be securely connected to the network. Once it has been connected, it is operational at the network layer, and its purpose is to perform application-layer onboarding (if needed). Once it has completed application-layer onboarding, its purpose is to execute its intended application. A device that is executing its application is operational at the application layer and is thereby achieving its ultimate purpose. When a device that has been operational at the application layer enters a maintenance phase, its purpose is to be updated and maintained as needed and then re-onboarded (if necessary) and made operational again.

This changing purpose of a device as it moves through its life cycle is relevant in terms of understanding what communications behavior should be expected and permitted of the device at various stages. A device's purpose changes as it moves through its life cycle, and its communications profile changes accordingly. The ability to enforce an evolving communications profile for a device ensures that the device communicates only in the ways that it is expected to communicate based on the phase of the onboarding process it is in at any given time. For example, a device that is not in its maintenance phase should not be expected or permitted to communicate with an update server. A device that is in its operational phase should not be expected or permitted to be provisioned with network-layer onboarding credentials. These should only be allowed to be received by the device during its initial network-layer onboarding or at the end of a maintenance phase that requires the device to be re-onboarded to the network layer.

Ideally, the onboarding solution's communications profile enforcement should be nuanced enough to enable the enforcement criteria to change depending on what phase of its life the device is in. An onboarding solution that could, for example, securely associate a device with a succession of MUD files would enable the network to enforce the communications requirements of the device that are particular to the device's purpose at any given phase in its life. For example, separate MUD files could be associated with the device for each of these phases in the device life:

- the period before the device has completed network-layer onboarding and connected to the network
- after the device has connected to the network but before it has completed application-layer onboarding
- after the device has completed application-layer onboarding but before it has begun executing its intended application and has thereby become operational at the application layer
- while the device is receiving software maintenance/updates
- while the device is receiving security maintenance/updates

- after the device has been decommissioned

For example, before the device performs network-layer onboarding, the device needs to perform bootstrapping and other steps to onboard and connect to the network, so it could be associated with a MUD file that permits only communications required to support this objective. At this point, the ultimate intent of the device beyond its mission to gain authorization to access the network is not relevant. The only operations the device should be performing during this phase are those required for it to onboard and connect.

Once the device has completed network-layer onboarding and has connected to the network, it could be associated with a different MUD file that expects it to perform only application-layer onboarding for the application indicated in the device's bootstrapping credentials. Once the device has completed application-layer onboarding, it could be associated with a new MUD file that expects it to perform its primary function. When a device enters a maintenance mode, it could be associated with yet another MUD file that no longer expects it to perform its primary function and instead expects the device to contact an update server, a security server, or some other entities, depending on the type of maintenance being performed (e.g., operating system patching, application upgrade, firmware upgrade, key rotation, certificate renewal). After a device is decommissioned, it would be associated with the same or a MUD file similar to the one with which it was associated before it performed its network-layer onboarding, with the expectation that it could be repurposed and so might have to undergo a new onboarding process.

6.4.23 Supply-chain security

Onboarding security, as with all device security, relies on supply-chain security. Supply-chain security, in general, refers to protection of a device as it moves through all initial phases of its life (e.g., 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. If a device manufacturer has supply-chain management tools and the onboarding solution can integrate with those tools, the manufacturer would be able to make supply-chain assurances regarding the trustworthiness of the devices used. If there were an issue with the supply chain (e.g., an integrator or other supplier no longer releases patches for a particular IoT device component) and the supply-chain management tool is integrated with the onboarding solution, such a supply-chain issue could, in theory, automatically be provided as information to a potential onboarding network, thereby preventing the device from being onboarded.

As mentioned in Section 6.4.9, a supply-chain compromise that can modify the X.509 certificate-based hardware credential that is installed in an IoT device will destroy the device's root of trust and thereby undermine operational security. For utmost security, it is crucial to ensure that IoT devices and network equipment that support onboarding be protected throughout the supply chain. If possible, assurances attesting to the integrity of firmware or other packages installed on a device should be supported, including software that has been installed by one or more system integrators, if possible. If system integrators are involved in the manufacturing process, they have to be trusted, and there should be a secure way of passing ownership and control of the device among system integrators and the manufacturer during the manufacturing process. Integration may involve the device being onboarded to several different integrator or manufacturer networks before it finishes the manufacturing process. After a device has been manufactured and sold, it is important that all suppliers and integrators continue to keep their components up-to-date and patched.

Integration of the IoT device onboarding solution with supply-chain management tools can provide assurances that devices are authentic, and their hardware, firmware, and software have not been tampered with or altered while in transit to the consumer. Device platform integrity can be ensured through mechanisms such as the abilities to trace and validate where and when every component of the IoT device platform was manufactured, to compare a snapshot of platform data and hashes computed during manufacturing with platform data and hashes computed at first boot, and to lock a device's boot process by having the manufacturer remove a password from the platform before the device is shipped. Therefore, the device will not be able to power up again until the password (which only the manufacturer and the consumer know) is replaced. Integration of IoT device onboarding solutions with supply-chain management tools can help ensure that only devices judged sufficiently trustworthy will be permitted to be onboarded.

7 Onboarding Use Cases

Below in Table 7-1 we enumerate onboarding characteristics appropriate for two general classes of use case for IoT device onboarding: consumer network and enterprise network. We want to be clear, however, that we are by no means asserting that these two use cases are always distinct from each other, that there are only two use cases, or that all consumer or all enterprise use cases are similar to one another. In some cases, a consumer network may require enterprise-class features. In many cases, consumers may desire to have enterprise-class security protections but face challenges in doing so. In other instances, a device may be built for consumers but be adopted by enterprises; a small business may be using consumer technology when it really needs enterprise-class capabilities. There is a continuum of requirements and solutions.

The enterprise use case type, especially, is by no means monolithic. Within the enterprise use case type are numerous different industry sector-specific use cases that differ from one another in nuanced ways. It will be important to define onboarding solution requirements and characteristics at a level of granularity that enables us to capture the unique facets that distinguish industry-sector use cases from one another. Some of the enterprise use case industry-sector verticals that have been identified so far are:

- industrial/manufacturing floor
- energy/oil and gas
- mining
- connected cities
- connected grids
- connected transportation
- carpeted space (e.g., office enterprise)
- nuclear (and other deployments in which devices may be sealed away for many years)
- education
- healthcare/medical

These industries may have different regulations, different risk factors, different sustainability or equipment availability requirements, and different certification processes. They may have different constraints regarding when and whether their IoT devices can be taken out of commission for upgrades, or their privacy issues may vary, among other things. This paper does not attempt to define the additional characteristics or granularity needed to distinguish among industry-specific verticals. However, we recognize the value in identifying ways to capture any differences, and we welcome input from stakeholders in these communities regarding their unique onboarding and security requirements.

Although the consumer/enterprise bifurcation of the use case space is overly simplistic, there still seems to be some value in understanding how the consumer and enterprise spaces compare in general, because there are certain clear distinctions. Table 7-1 lists our best understanding of how the consumer and general enterprise network use cases differ with respect to the relevant

1904 characteristics that were identified in Section 6.

1905 **Table 7-1 Consumer Versus General Enterprise Use Case Characteristics**

Attribute/Capability	Consumer Network	Enterprise Network
ease of use	required. Solution works easily out of the box without needing a trained operator.	desirable but not required. Can assume availability of a trained operator with security and technical experience
network access technology	Wi-Fi, perhaps some wired	wired, Wi-Fi, LTE, 5G
infrastructure dependencies	minimize need for additional network components required to be installed or available to support the solution	Solution may require additional components and more robust infrastructure (e.g., an authorization service and a security information and event management component will be available to support more elaborate solutions).
ease of integration into existing environment	minimize changes required to existing home network	can tolerate a little more change to existing enterprise environment if needed
number of new components introduced	the fewer the better	can tolerate additional infrastructure components if needed
cost of required network infrastructure	very low cost desired	can tolerate higher cost if needed
cost of IoT devices	very low cost desired	low cost desired
discovery-initiated onboarding	desirable	desirable
hands-free (zero-touch)	Desirable, but some manual intervention is okay if it is very easy for the user.	required for purposes of bulk onboarding
bulk onboarding	not required. The home network has fewer devices overall, and these are not typically onboarded at the same time.	required. Many devices will potentially need to be set up at once, without user intervention.
proof of ownership	not required	desirable for strong security
onboard without internet access	may be required in some cases	may be required in some cases
provision of application data	may need to provision application-level data to the device after network-layer onboarding	more likely to be able to provision application-level data to the device after network-layer onboarding
device accessibility requirements	It will not typically be a challenge to have devices accessible.	Accessibility may sometimes be a challenge.
deployment challenges	There should be none. Onboarding should be seamless.	Some may be tolerated if the typical IT professional can address them.
standards-based or proprietary	Standards-based solution is preferred to avoid reduced choice and increased costs that could result from being locked into a proprietary ecosystem.	Standards-based solution is required.
regulatory compliance	not typically of concern	Regulatory compliance is mandatory for certain industry sectors.
certification program	desirable to provide consumer guidance and peace of mind	desirable; may be required in some cases

Attribute/Capability	Consumer Network	Enterprise Network
sustainability	desirable but not mandatory	desirable; may be required in some cases
threats	phishing attacks, exploitation of well-known vulnerabilities	phishing, exploitation of well-known vulnerabilities, industrial espionage, insider threat
Security Characteristics	Security-related distinctions between the two use cases have not been considered.	

8 A Set of Recommended Security Capabilities for Onboarding

The level of security that is provided during onboarding depends on the characteristics of the onboarding solution used. Is it possible to agree on the minimum-security characteristics for an onboarding solution? In regulated industries, the law may mandate security baselines. In some cases, the requirements will depend on the criticality of the data that the IoT device will handle. NIST is developing some IoT security baselines that will apply minimum security recommendations to devices installed in U.S. government environments. NIST has also published NIST Interagency or Internal Report (NISTIR) 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [20] ; and NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [21], which defines a baseline of core cybersecurity capabilities that manufacturers can voluntarily adopt for IoT devices that they produce. This baseline is intended to address general cybersecurity risks faced by a generic customer by serving as a default voluntary guideline for minimally securable IoT devices. It identifies six core baseline cybersecurity capabilities that should be supported, along with associated common elements that an organization seeking to implement the core baseline often (but not always) would use to achieve the capability. Each feature and key element in the core baseline stems directly from the contents of Section 4 of NISTIR 8228 [22], *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. The European Telecommunications Standards Institute (ETSI) has also published ETSI EN 303 645, *Cyber Security for Consumer Internet of Things: Baseline Requirements* [23], a standard for cybersecurity in IoT that establishes a security baseline for internet-connected consumer products and provides a basis for future IoT certification schemes.

Using these NIST and ETSI IoT security documents as background, Table 8-1 defines a proposed set of recommended security capabilities for onboarding solutions. Each onboarding security characteristic that was enumerated in Table 6-4 is listed in the first column of Table 8-1. For each onboarding security characteristic listed in the first column, a related recommended security capability is proposed in the second column. The third column specifies recommendations for the characteristic to guide implementation. The rationale for each security capability is provided in the fourth column. The rationale may be derived from material found in NISTIR 8259A or ETSI EN 303 645, in which case this is made clear, and the cybersecurity feature or provision to which the value can be traced is listed. When the fourth column value does not cite either NISTIR 8259A or ETSI EN 303 645 for a given security characteristic, it indicates that the rationale for the proposed value in column two cannot be directly traced to any cybersecurity feature in NISTIR 8259A or any provision in ETSI EN 303 645. In these cases, the values we have proposed in column two represent our initial best effort at defining a set of security capabilities that makes sense.

The intention of this section is to present a proposed set of recommended security capabilities for a generic onboarding solution. It introduces the recommendations to elicit feedback from community stakeholders to better understand the factors that should be considered. The set of security capabilities presented in Table 8-1 is meant to be general and as such does not include any industry-sector-specific nuances or regulations.

Table 8-1 Proposed Set of Recommended Security Capabilities of an Onboarding Solution

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.	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.	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 device's actual identity.	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 a way that it is protected from unauthorized access and modification, such as in a cryptographic module.	NISTIR 8259A: core baseline data protection capability. ETSI EN 303 645: Provisions 5.5-4 and 5.5-5

Characteristic	Proposed Set of Recommended Security Capabilities	Recommendations	NISTIR Document Derivation or Other Rationale
device authorization	no capability currently recommended	The onboarding solution should support device authorization through integration with an authorization service (esp. for enterprise solutions) and/or by conveying the device's MUD URL to the network.	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.	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

Characteristic	Proposed Set of Recommended Security Capabilities	Recommendations	NISTIR Document Derivation or Other Rationale
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).	
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 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).	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 from the device, it should not be possible to delete the device's bootstrapping 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

Characteristic	Proposed Set of Recommended Security Capabilities	Recommendations	NISTIR Document Derivation or Other Rationale
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.
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.	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.	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).

Characteristic	Proposed Set of Recommended Security Capabilities	Recommendations	NISTIR Document Derivation or Other Rationale
connected device and onboarded device cross-check	no capability currently recommended	It would be desirable for the onboarding solution to integrate with centralized asset management systems to support this cross-check capability. However, not all devices will necessarily be able to participate in the centralized asset management system, which would mean that they would not be able to benefit from this capability even if it were available.	NISTIR 8228: Table 1, item 2, "The IoT device may not be able to participate in a centralized asset management system."
supply-chain security	no capability currently recommended	Integration of supply-chain management tools with the onboarding solution can provide supply-chain assurances regarding the trustworthiness of devices as an input to onboarding decisions.	
proof of ownership	no capability currently recommended	Proof-of-ownership verification enables IoT devices to compare device ownership information with network ownership information before they allow themselves to be onboarded (and thereby taken over) by a network.	
secure ownership transfer	no capability currently recommended	Secure ownership transfer is required to maintain accurate device ownership information and supply-chain security.	
onboard only to authorized networks	no capability currently recommended	Onboarding solutions that support "onboard only to authorized networks" mechanisms enable IoT devices to ensure that they will be onboarded only to networks that their owner has authorized. Such mechanisms are dependent on both proof-of-ownership verification and secure ownership transfer.	

Characteristic	Proposed Set of Recommended Security Capabilities	Recommendations	NISTIR Document Derivation or Other Rationale
privacy	All information (e.g., the device's network credentials) stored on the device post-manufacturing can be deleted by authorized personnel. If an onboarding mechanism uses a device information declaration (or similar mechanism), this device information declaration should be encrypted both while it is in transit and while it is stored, to prevent unauthorized disclosure of personal information related to the device owner and the device's authorized onboarders.	If the IoT device logs and stores cybersecurity events locally, these logs can be deleted by an authorized entity (e.g., in preparation for the device being resold). If the IoT device stores the device's cybersecurity state locally, this state can be deleted by an authorized entity (e.g., in preparation for the device being resold).	NISTIR 8259A: core baseline data protection capability. ETSI EN 303 645: Provisions 5.8 and 5.11
MUD support	The onboarding solution supports conveyance of a MUD URL from the device to the network.	The onboarding solution should strongly bind the MUD URL to the device's identity, and it should maintain the confidentiality of the MUD URL while it is in transit to the network. Support for MUD URL conveyance enables the onboarding solution to integrate with the network's MUD capabilities, thereby ensuring that the local network can enforce the IoT device's intended communications profile. MUD enables access to each of the device's network interfaces to be restricted according to certain protocols, ports, other local devices, and internet destinations. In particular, MUD enables the entities that are permitted to update the IoT device's onboarding and other software and firmware to be restricted to authorized entities only. MUD also enables the other components to which the IoT device is permitted to send traffic to be restricted.	NISTIR 8259A: core baseline device identification capability (device intent signaling is mentioned in the rationale for this capability but is not included as part of the baseline requirements)
evolving communications profile enforcement	no capability currently recommended	The ability to enforce an evolving communications profile is only a theoretical capability at this time.	
regulatory compliance	N/A	The proposed recommended security capabilities do not imply compliance with any specific industry-sector regulations.	

1949

9 Next Steps

We would like to receive feedback on this document from all stakeholders. The NCCoE plans to leverage this content to drive development of a potential NCCoE project focused on enhancing IoT device security through trusted network-layer onboarding. Whether you are a user, device manufacturer, service provider, or other stakeholder, we are interested in understanding more about your use case and learning what onboarding characteristics must be supported to meet its requirements. In particular, we seek:

- Users–please provide us with a description of the requirements for onboarding in your environment or industry vertical by providing the following feedback:
    - what security characteristics in Table 6-4 your onboarding solution must support
    - what onboarding characteristics in Table 6-1 are relevant to your use case
    - what values for each characteristic in Table 7-1 best apply to your use case
    - suggestions for additional characteristics that may not be listed
    - what onboarding solution characteristics are required to support your industry vertical's use case, what characteristics are nice to have but are optional, and what characteristics you do not need or even want
    - whether the security capabilities for onboarding provided in Table 8-1 meet your security requirements
    - any additional information you wish to provide
- IoT device manufacturers–using the characteristics listed in Table 6-2 and Table 6-4 as a guide, please provide the following feedback:
    - what characteristics must be common across all onboarding solutions and what characteristics may be present only optionally
    - suggestions for additional characteristics that may not be listed
    - whether the security capabilities for onboarding provided in Table 8-1 meet your security requirements
    - what other application-layer onboarding examples should be included
    - any additional information you wish to provide
- Service providers–using the characteristics listed in Table 6-3 and Table 6-4 as a guide, please provide the following feedback:
    - what characteristics are not negotiable and must be present. For example, are you unwilling to accept the use of pre-shared keys?
    - regarding the cost characteristic, how we can best quantify this
    - suggestions for additional characteristics that may not be listed
    - whether the security capabilities for onboarding provided in Table 8-1 meet your security requirements
    - any additional information you wish to provide

Please share your viewpoint.

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
CDI	Compound Device Identifier
CRL	Certificate Revocation List
DAA	Direct Anonymous Attestation
DICE	Device Identifier Composition Engine
DPP	Device Provisioning Protocol
eSIM	embedded subscriber identity module
ETSI	European Telecommunications Standards Institute
ID	Identifier
IDE	Integrated Development Environment
IoT	Internet of Things
IP	Internet Protocol
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
ISP	internet service providers
IT	Information Technology
JSON	JavaScript Object Notation
MAC	Media Access Control
MUD	Manufacturer Usage Description
NCCoE	National Cybersecurity Center of Excellence

NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
OOB	Out of Band
PSK	Pre-Shared Key
RFC	Request for Comments
R&D	Research and Development
SSID	Service Set Identifier
TPM	Trusted Platform Module
URL	Uniform Resource Locator
WPS	Wi-Fi Protected Setup

1992 # Appendix B—References

[1] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (January 23, 2013) Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack, Alert (TA12-006A). Available at https://www.us-cert.gov/ncas/alerts/TA12-006A

[2] Thakore D, (April 9, 2019) Micronets Deep Dive, National Cybersecurity Center of Excellence, Mitigating IoT-Based DDoS meeting, Rockville, MD, unpublished.

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

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

[5] Pandey AK (2019) AutoAdd—Automatic Bootstrapping of IoT Devices. (Internet Engineering Task Force [IETF]). https://tools.ietf.org/html/draft-autoadd-auto-bootstrapping-iot-devices-00

[6] Sarikaya B, Sethi M, Garcia-Carrillo D (2019) Secure IoT Bootstrapping: A Survey. (IETF Network Working Group). https://www.ietf.org/id/draft-sarikaya-t2trg-sbootstrapping-08.txt

[7] Thakore D (November 4, 2019) IoT Device Onboarding & Lifecycle Management presentation, slide 9. (IoT Device Onboarding & Lifecycle Management meeting, Washington, DC, unpublished.

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

[9] Watsen K, Richardson M, Pritikin M, Eckert T (2018) A Voucher Artifact for Bootstrapping Protocols. (IETF), IETF Request for Comments (RFC) 8366. https://tools.ietf.org/html/rfc8366#:~:text=RFC%208366%20Voucher%20Profile%20May%202018%20Ownership%20ID,after%20the%20inclusion%20of%20a%20registrar%20ID%20wildcard.

[10] Vermillard J (2015) Bootstrapping device security with Lightweight M2M. https://medium.com/@vrmvrm/device-key-distribution-with-lightweight-m2m-36cdc12e5711

[11] Garcia-Morchon O, Kumar S, Sethi M (2019) Internet of Things (IoT) Security: State of the Art and Challenges. (Internet Research Task Force [IRTF]), IRTF RFC 8576. https://tools.ietf.org/html/rfc8576#:~:text=RFC%208576%20IoT%20Security%20April%202019%20operational%20mode,several%20years%2C%20occasional%20maintenance%20cycles%20may%20be%20required.

[12] Atkinson S (December 7, 2017) IoT and connected device lifecycle management. (CIO). https://www.cio.com/article/3241264/iot-and-connected-device-lifecycle-management.html

[13] Abhishek A (November 4, 2019) IoT Device Onboarding & Lifecycle Management. Cisco Systems IoT Device Onboarding & Lifecycle Management meeting, Washington, DC, unpublished

[14] Boyens J, Paulsen C, Moorthy R, Bartol N (2020) NIST Special Publication 800-161 Rev. 1 (Draft), *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* (NIST, Gaithersburg, MD). https://csrc.nist.gov/publications/detail/sp/800-161/final

[15] IEEE (2018) IEEE 802.1AR-2018—IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity. (IEEE). https://standards.ieee.org/standard/802_1AR-2018.html

[16] Trusted Computing Group (2018) Hardware Requirements for a Device Identifier Composition Engine, Family 2.0, Level 00 Revision 78. (Trusted Computing Group). https://trustedcomputinggroup.org/wp-content/uploads/Hardware-Requirements-for-Device-Identifier-Composition-Engine-r78_For-Publication.pdf

[17] Chandler M (2017) Intel Enhanced Privacy ID (EPID) Security Technology. (Intel). https://software.intel.com/en-us/articles/intel-enhanced-privacy-id-epid-security-technology

[18] Global System for Mobile Communications Association (GSMA) (2018) eSIM Whitepaper: The what and how of Remote SIM Provisioning. (GSMA). https://www.gsma.com/esim/wp-content/uploads/2018/06/eSIM-Whitepaper-v4.11.pdf

[19] Arm Limited (2020) Entity Attestation Token White Paper: How Service Providers can Trust the Internet of Things Version: 1. (Arm Limited). https://www.psacertified.org/app/uploads/2020/02/PSA_Certified_Entity_Attestation_Overview_Whitepaper.pdf

[20] Fagan M, Megas KN, Scarfone K, Smith M (2020) National Institute of Standards and Technology (NIST) Interagency or Internal Report (IR) 8259, *Foundational*

Cybersecurity Activities for IoT Device Manufacturers. (NIST, Gaithersburg, MD). https://csrc.nist.gov/publications/detail/nistir/8259/final

[21] Fagan M, Megas KN, Scarfone K, Smith M (2020) NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*. (NIST, Gaithersburg, MD). https://csrc.nist.gov/publications/detail/nistir/8259a/final

[22] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas KN, Nadeau E, O'Rourke DG, Piccarreta B, Scarfone K (2019) NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. (NIST, Gaithersburg, MD). https://csrc.nist.gov/publications/detail/nistir/8228/final

[23] ETSI EN 303 645, V2.1.1, *Cyber Security for Consumer Internet of Things: Baseline Requirements*. (European Telecommunications Standards Institute, Sophia Antipolis Cedex – FRANCE). https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf