PROJECT DESCRIPTION

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

Enhancing Internet Protocol-Based IoT Device and Network Security

Paul Watrobski
Murugiah Souppaya

Information Technology Laboratory
National Institute of Standards and Technology

Susan Symington
Parisa Grayeli
Joshua Klosterman
Blaine Mulugeta

The MITRE Corporation

William C. Barker

Dakota Consulting

DRAFT

March 2021

iot-onboarding@nist.gov

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

Abstract

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

Acknowledgment

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

Keywords

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

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to iot-onboarding@nist.gov.

Public comment period: March 16, 2021 to April 19, 2021

TABLE OF CONTENTS

1 Executive Summary

Purpose

Network-layer onboarding of an Internet of Things (IoT) device is the provisioning of network credentials to that device. Network credentials are needed so that only authorized devices can connect to and use an organization's networks. However, the established approaches to network-layer onboarding for IoT devices all have major challenges:

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

A different approach to secure onboarding that avoids these flaws is needed. The desired process, called *trusted network-layer onboarding*, would be an automated approach with these characteristics:

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

Trusted network-layer onboarding could provide assurance that a network is not put at risk as new IoT devices are added to it and also safeguard IoT devices from being taken over by unauthorized networks.

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

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

Scope

The project encompasses trusted network-layer onboarding of IoT devices deployed across different internet protocol-based environments using wired, Wi-Fi, and broadband networking technologies. The scope also includes additional security capabilities that can be integrated with and enhanced by the onboarding mechanism to protect the device and the network to which it connects throughout the device's lifecycle.

Assumptions/Challenges

As with any other device, an IoT device needs appropriate credentials in order to connect to a network securely. A typical commercially available, mass-produced IoT device is built to be identical regardless of its intended customer and is not pre-provisioned with unique network credentials during the manufacturing process. To take advantage of economies of scale and to avoid the risk of providing manufacturers with access to the device's local network credentials, these credentials are provisioned to the device at the time of the device's deployment on the network.

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

Other networks use a more robust security model that requires each device to have its own distinct credential to connect. However, this often means that the onboarding process is complex, resource intensive, and possibly error prone. If the process requires individuals to have access to device credentials, such access makes those credentials more vulnerable to being disclosed to unauthorized parties. In order to be zero-touch, most trusted onboarding solutions 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 [1]. This effectively requires a manufacturer to uniquely configure individual devices to customize onboarding credentials for each customer use case on a build-to-order basis, which is inefficient and expensive. The complexity of customizing each device's onboarding credentials during the device manufacturing process in this manner, combined with the fact that it is susceptible to human error, make it vulnerable to security risks [2].

This NCCoE project description builds on the documentary research presented in the NIST Draft Cybersecurity White Paper: Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management [3]. The paper describes key concepts and characteristics for a trusted onboarding solution in addition to other capabilities like device attestation, device intent, asset management, etc. The trusted onboarding characteristics that we will try to demonstrate in this project will be discussed later in the Desired Capabilities Section.

2 Scenarios

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

Scenario 1: Trusted network-layer onboarding

This scenario involves trusted network-layer onboarding of an authorized IoT device directly to an authorized network, as performed after the device has booted up and is placed in onboarding mode. In this scenario, after the identities of the device and the network are authenticated, the network provisions unique network credentials to the device over a secure channel. The device then uses these credentials to connect to the network.

Scenario 2: Validation of device authenticity and integrity

This scenario involves performing attestation, supply chain management (e.g., hardware, firmware, and software component inventory), configuration monitoring, or other asset-management-related operations on an IoT device to validate its authenticity and integrity. These operations may be performed before permitting the device to be onboarded to the network, and they may also be performed on an ongoing basis after the device is onboarded and connected to the network.

Scenario 3: Trusted application-layer onboarding

This scenario involves trusted application-layer onboarding that is performed automatically on an IoT device after it connects to a network. As a result, this scenario can be thought of as a series of steps that would be performed as an extension of scenario 1.

Scenario 4: Re-onboarding a wiped device

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

Scenario 5: Onboarding with device intent enforcement

This scenario involves onboarding an IoT device to a network, augmented with a mechanism for device intent enforcement (for example, MUD [4]). This could include secure communication of device intent data, assignment of the IoT device to a separate subnetwork, ongoing support for device intent enforcement after the device connects to the network, and use of a local device intent policy that permits the IoT device to communicate with an endpoint even though permission to communicate with that endpoint is not explicitly granted.

3 High-Level Architecture

Logical Architecture

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

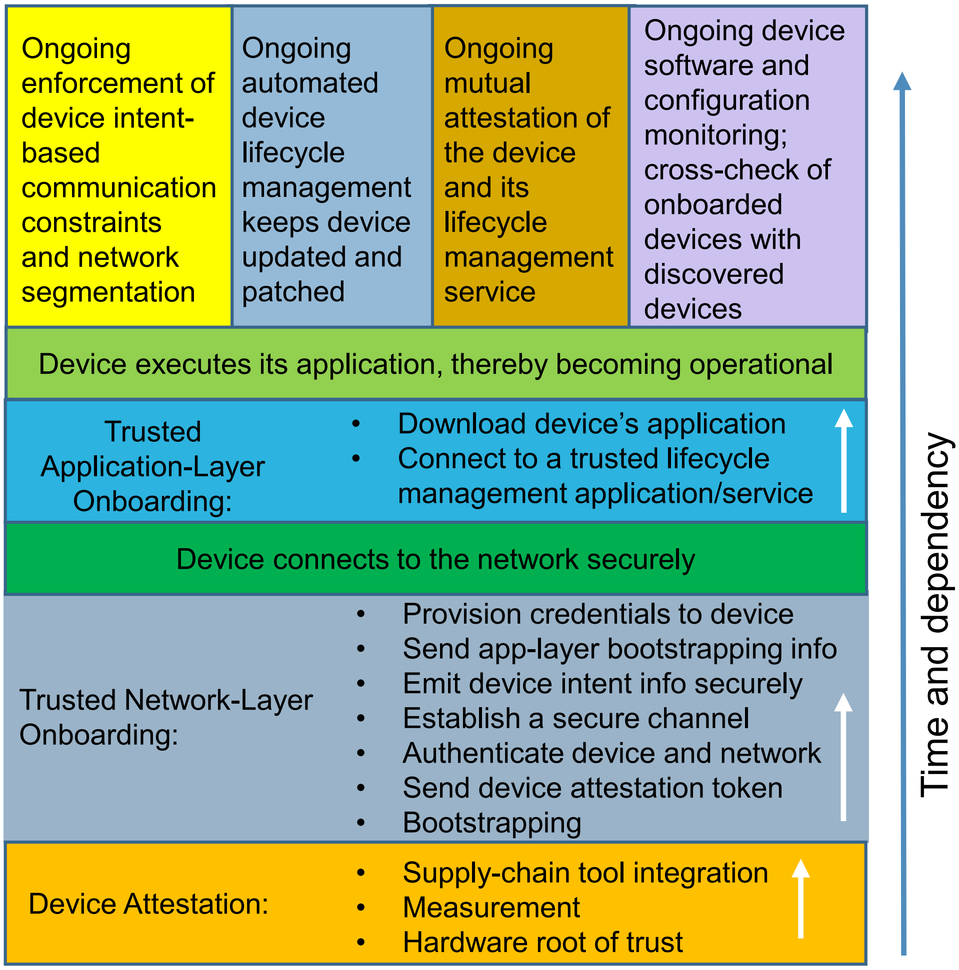

Figure 1: Dependency Chain of Protection Mechanisms

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

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

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

While the device is operational, a number of processes can be performed on an ongoing basis to ensure continued security throughout the device's lifecycle. Examples include the following:

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

High-Level Solution Architecture

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

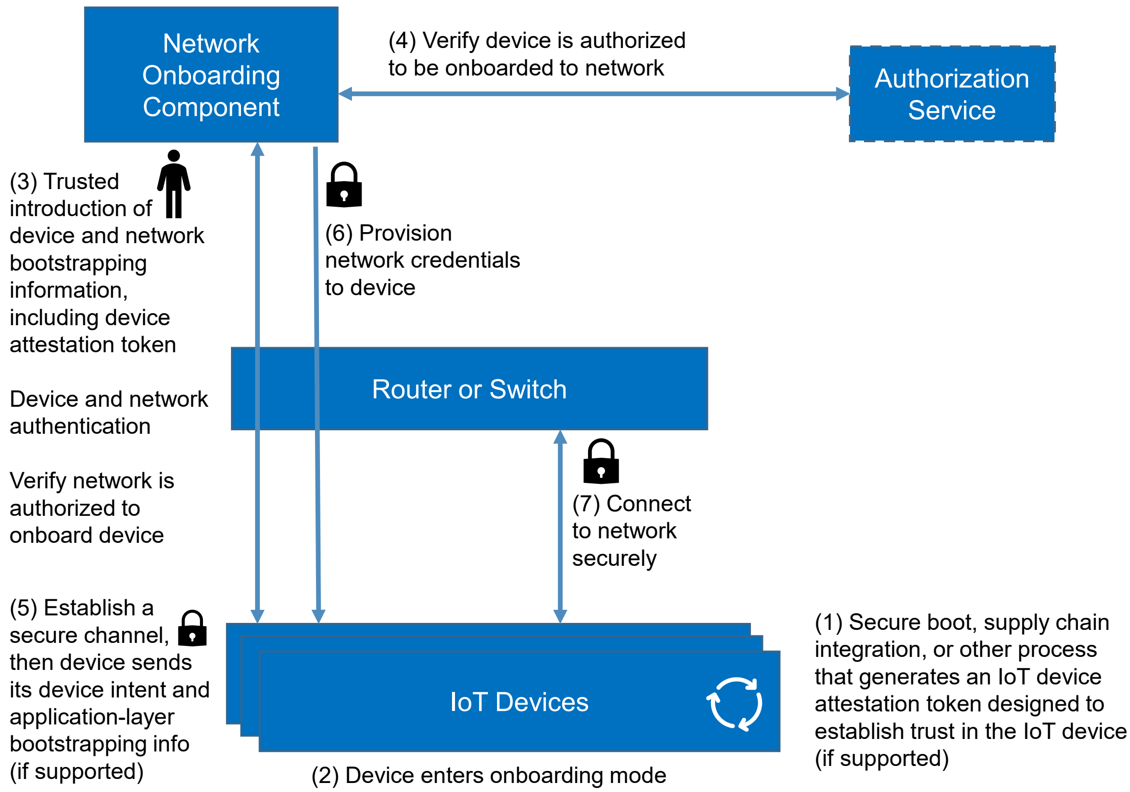

Figure 2: Notional High-Level Architecture

The following summarizes possible steps in trusted network-layer onboarding based on the Figure 2 architecture. The numbered items correspond to the numbers in the figure.

1. This is an optional step that is not part of trusted onboarding. If the device and the onboarding solution support attestation, the IoT device generates or receives a signed attestation token that makes claims about the device (e.g., device ID, manufacturer, model, installed software, versions, boot state, measurements, integrity checks of running hardware and firmware/software). This step might involve integration with supply-chain management tools that can provide assurance that devices are authentic and that their hardware, firmware, and software has not been tampered with or altered.
2. The IoT device to be onboarded is placed in onboarding mode, i.e., it is put into a state such that it is actively listening for and able to send onboarding protocol messages.
3. Bootstrapping is performed to provide a trusted introduction of the device to the network and of the network to the device. Using the device and network bootstrapping credentials that were provided via the trusted introduction, the network authenticates the identity of the IoT device and the IoT device authenticates the identity of the network. The device also verifies that the network is authorized to onboard it. The device sends the signed device attestation token that it had generated in step 1 to the network onboarding component.
4. The network onboarding component consults the network's authorization service to verify that the device is authorized to be onboarded to the network.

5. A secure channel is established between the network onboarding component and the device. If supported, the device uses the secure channel to send device intent and application-layer bootstrapping information to the network.
6. The network onboarding component uses the secure channel to send the device its network credentials.
7. The device uses its newly provisioned credentials to securely connect to the network.

Component List

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

- **IoT devices**: Each device must be able to participate in trusted network-layer onboarding and to securely store private keys, credentials, and other information. Each device may have other capabilities that enable its use with additional solution components, such as the examples listed below.
- **Network onboarding component**: The network onboarding component must be able to interact with the IoT devices on behalf of the network via the network-layer onboarding protocol.
- **Authorization service**: The authorization service must be able to determine which IoT devices are authorized to be onboarded to the network and maintain a record of onboarded devices.
- **Router or switch**: The router or switch must be able to route all traffic exchanged between the IoT devices and the rest of the network.

In addition, the architecture may contain several types of additional components, none of which are depicted in Figure 2:

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

Desired Capabilities

The following are desired capabilities for a trusted network-layer onboarding solution. They are drawn from the list and definitions in [3]. Note that this list does not include additional capabilities beyond the trusted network-layer onboarding solution itself, such as application-layer onboarding and ongoing device lifecycle management protections. See the “Logical Architecture” section of this document for more information on these capabilities.

Device Identity Management, Authentication, and Access Control:

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

Network Identity Management, Authentication, and Access Control:

- The solution provides the identifier of the network to which the device should connect as part of the onboarding credentials that it provisions.
- The solution verifies that the network’s asserted identity is its actual identity.
- The solution enables the device to verify that the network is authorized to take control of the device before the device allows itself to be onboarded.

Data Protection:

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

4 Relevant Standards and Guidance

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

- Wi-Fi Alliance, *Draft Device Provisioning Protocol Specification Version 1.2*, 2020. https://www.wi-fi.org/file/device-provisioning-protocol-draft-specification [membership required]
- M. Pritikin, M. Richardson, T.T.E. Eckert, M.H. Behringer, and K.W. Watsen, *Bootstrapping Remote Secure Key Infrastructures (BRSKI)*, Nov. 2020. https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
- G. Cooper et al (editors), *FIDO Device Onboard Specification, Review Draft,* FIDO Alliance, Dec. 2020. https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.0-20201202.pdf

- M. Fagan, K.N. Megas, K. Scarfone, and M. Smith, *IoT Device Cybersecurity Capability Core Baseline,* National Institute of Standards and Technology, NISTIR 8259A, May 2020. https://doi.org/10.6028/NIST.IR.8259A
- ETSI EN 303 645, V2.1.1 (2020-06), *Cyber Security for Consumer Internet of Things: Baseline Requirements*, European Telecommunications Standards Institute, June 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- G. Mandyam, L. Lundblade, M. Ballesteros, and J. O'Donoghue, *The Entity Attestation Token (EAT)*, IETF Remote Attestation Procedures Working Group, Feb. 2021. Available: https://tools.ietf.org/html/draft-ietf-rats-eat-07

Appendix A References

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

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

[3] S. Symington, W. Polk, and M. Souppaya, *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management (Draft)*, National Institute of Standards and Technology (NIST) Draft Cybersecurity White Paper, Gaithersburg, MD, Sept. 2020, 85 pp. https://doi.org/10.6028/NIST.CSWP.09082020-draft

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