NIST SPECIAL PUBLICATION 1800-36D

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

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume D:
Functional Demonstrations

Paul Watrobski
Murugiah Souppaya
National Cybersecurity Center of Excellence
Information Technology Laboratory

Andy Dolan
Kyle Haefner
Craig Pratt
Darshak Thakore
CableLabs,
Louisville, Colorado

Brecht Wyseur
Kudelski IoT, Cheseaux-sur-Lausanne,
Switzerland

Nick Allott
Ashley Setter
Nquiring Minds
Southampton, United Kingdom

Michael Richardson
Sandleman Software Works
Ontario, Canada

Mike Dow
Steve Egerter
Silicon Labs,
Austin, Texas

Chelsea Deane
Joshua Klosterman
Blaine Mulugeta
Charlie Rearick
Susan Symington
The MITRE Corporation
McLean, Virginia

May 2024

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-36D, Natl. Inst. Stand. Technol. Spec. Publ. 1800-36D, 51 pages, May 2024, CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Public comment period: May 31, 2024 through July 30, 2024

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

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 issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

KEYWORDS

application-layer onboarding; bootstrapping; Internet of Things (IoT); Manufacturer Usage Description (MUD); network-layer onboarding; onboarding; Wi-Fi Easy Connect.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Amogh Guruprasad Deshmukh	Aruba, a Hewlett Packard Enterprise company
Dan Harkins	Aruba, a Hewlett Packard Enterprise company
Danny Jump	Aruba, a Hewlett Packard Enterprise company
Bart Brinkman	Cisco
Eliot Lear	Cisco
Peter Romness	Cisco
Tyler Baker	Foundries.io
George Grey	Foundries.io
David Griego	Foundries.io
Fabien Gremaud	Kudelski IoT
Faith Ryan	The MITRE Corporation
Toby Ealden	NquiringMinds
John Manslow	NquiringMinds
Antony McCaigue	NquiringMinds
Alexandru Mereacre	NquiringMinds
Loic Cavaille	NXP Semiconductors
Mihai Chelalau	NXP Semiconductors
Julien Delplancke	NXP Semiconductors
Anda-Alexandra Dorneanu	NXP Semiconductors

Name	Organization
Todd Nuzum	NXP Semiconductors
Nicusor Penisoara	NXP Semiconductors
Laurentiu Tudor	NXP Semiconductors
Michael Richardson	Sandelman Software Works
Karen Scarfone	Scarfone Cybersecurity
Steve Clark	SEALSQ, a subsidiary of WISeKey
Pedro Fuentes	SEALSQ, a subsidiary of WISeKey
Gweltas Radenac	SEALSQ, a subsidiary of WISeKey
Kalvin Yang	SEALSQ, a subsidiary of WISeKey

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Collaborators		
Aruba, a Hewlett Packard Enterprise company	Kudelski IoT	Sandelman Software Works
CableLabs	NquiringMinds	Silicon Labs
Cisco	NXP Semiconductors	SEALSQ, a subsidiary of WISeKey
Foundries.io	Open Connectivity Foundation (OCF)	

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: iot-onboarding@nist.gov.

Contents

1 Introduction...1
1.1 How to Use This Guide...1
2 Functional Demonstration Playbook 3
2.1 Scenario 0: Factory Provisioning 3
2.2 Scenario 1: Trusted Network-Layer Onboarding...4
2.3 Scenario 2: Trusted Application-Layer Onboarding...5
2.4 Scenario 3: Re-Onboarding a Device...6
2.5 Scenario 4: Ongoing Device Validation 7
2.6 Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle 8
3 Functional Demonstration Results 9
3.1 Build 1 Demonstration Results...9
3.2 Build 2 Demonstration Results...16
3.3 Build 3 Demonstration Results...22
3.4 Build 4 Demonstration Results...28
3.5 Build 5 Demonstration Results...34
Appendix A References 42

List of Tables

Table 2-1 Scenario 0 Factory Provisioning Capabilities That May Be Demonstrated 4
Table 2-2 Scenario 1 Trusted Network-Layer Onboarding Capabilities That May Be Demonstrated 5
Table 2-3 Scenario 2 Trusted Application-Layer Onboarding Capabilities That May Be Demonstrated .. 6
Table 2-4 Scenario 3 Re-Onboarding Capabilities That May Be Demonstrated 6
Table 2-5 Scenario 4 Ongoing Device Validation Capabilities That May Be Demonstrated 7
Table 2-6 Scenario 5 Credential and Device Posture Establishment and Maintenance Capabilities That May Be Demonstrated 8
Table 3-1 Build 1 Capabilities Demonstrated 9
Table 3-2 Build 2 Capabilities Demonstrated 16
Table 3-3 Build 3 Capabilities Demonstrated 22
Table 3-4 Build 4 Capabilities Demonstrated 28

Table 3-5 Build 5 Capabilities Demonstrated 35

1 Introduction

In this project, the National Cybersecurity Center of Excellence (NCCoE) is applying standards, recommended practices, and commercially available technology to demonstrate various mechanisms for trusted network-layer onboarding of IoT devices and lifecycle management of those devices. We show how to provision network credentials to IoT devices in a trusted manner and maintain a secure posture throughout the device lifecycle.

This volume of the NIST Cybersecurity Practice Guide describes functional demonstration scenarios that are designed to showcase the security capabilities and characteristics supported by trusted IoT device network-layer onboarding and lifecycle management solutions. Section 2, Functional Demonstration Playbook, defines the scenarios and lists the capabilities that can be showcased in each one. Section 3, Functional Demonstration Results, reports which capabilities have been demonstrated by each of the project's implemented solutions.

1.1 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design for implementing trusted IoT device network-layer onboarding and lifecycle management and describes various example implementations of this reference design. Each of these implementations, which are known as *builds,* is standards-based and is designed to help provide assurance that networks are not put at risk as new IoT devices are added to them, and also to help safeguard IoT devices from being taken over by unauthorized networks. The reference design described in this practice guide is modular and can be deployed in whole or in part, enabling organizations to incorporate trusted IoT device network-layer onboarding and lifecycle management into their legacy environments according to goals that they have prioritized based on risk, cost, and resources.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed.

This guide contains five volumes:

- NIST SP 1800-36A: *Executive Summary* – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-36B*: Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-36C: *How-To Guides* – instructions for building the example implementations, including all the security-relevant details that would allow you to replicate all or parts of this project
- NIST SP 1800-36D: *Functional Demonstrations* – use cases that have been defined to showcase trusted IoT device network-layer onboarding and lifecycle management security capabilities, and the results of demonstrating these use cases with each of the example implementations **(you are here)**
- NIST SP 1800-36E*: Risk and Compliance Management* – risk analysis and mapping of trusted IoT device network-layer onboarding and lifecycle management security characteristics to cybersecurity standards and recommended practices

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-36A*, which describes the following topics:

- challenges that enterprises face in migrating to the use of trusted IoT device network-layer onboarding
- example solutions built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-36B*, which describes what we did and why.

Also, Section 4 of *NIST SP 1800-36E* will be of particular interest. Section 4, *Mappings*, maps logical components of the general trusted IoT device network-layer onboarding and lifecycle management reference design to security characteristics listed in various cybersecurity standards and recommended practices documents, including *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) and *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53).

You might share the *Executive Summary, NIST SP 1800-36A*, with your leadership team members to help them understand the importance of using standards-based trusted IoT device network-layer onboarding and lifecycle management implementations.

IT professionals who want to implement similar solutions will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-36C*, to replicate all or parts of the builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution. Also, you can use *Functional Demonstrations, NIST SP 1800-36D*, which provides the use cases that have been defined to showcase trusted IoT device network-layer onboarding and lifecycle management security capabilities and the results of demonstrating these use cases with each of the example implementations. Finally, *NIST SP 1800-36E* will be helpful in explaining the security functionality that the components of each build provide.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a trusted IoT device network-layer onboarding and lifecycle management solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and recommended practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. We seek feedback on the publication's contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to iot-onboarding@nist.gov.

2 Functional Demonstration Playbook

Six scenarios have been defined that demonstrate capabilities related to various aspects of trusted IoT device network-layer onboarding, application-layer onboarding, and device lifecycle management. These scenarios are as follows:

- Scenario 0: Factory Provisioning
- Scenario 1: Trusted Network-Layer Onboarding
- Scenario 2: Trusted Application-Layer Onboarding
- Scenario 3: Re-Onboarding a Device
- Scenario 4: Ongoing Device Validation
- Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle

We executed the factory provisioning scenario (Scenario 0) using both a Bootstrapping Remote Secure Key Infrastructure (BRSKI) Factory Provisioning Build and a Wi-Fi Easy Connect Factory Provisioning Build that have been implemented as part of this project. We executed the trusted network-layer onboarding and lifecycle management scenarios using each of the onboarding builds that have been implemented as part of this project. The capabilities that were demonstrated depend both on the features of the network-layer onboarding protocol (i.e., Wi-Fi Easy Connect) that the build supports and on any additional mechanisms the build may have integrated (e.g., application-layer onboarding).

Section 2.1 defines the factory provisioning scenario (Scenario 0). Sections 2.2 through Section 2.6 define each of the five onboarding scenarios.

2.1 Scenario 0: Factory Provisioning

This scenario, which simulates the IoT device factory provisioning process, is designed to represent some steps that must be performed in the factory before the device is put into the supply chain. These steps are performed by the device manufacturer or integrator to provision a device with the information it requires to be able to participate in trusted network-layer onboarding and lifecycle management. The device is assumed to have been equipped with secure storage and with the software or firmware needed to support a specific network-layer onboarding protocol (e.g., Wi-Fi Easy Connect or BRSKI). Scenario 0 includes initial provisioning of the IoT device with its birth credential (e.g., its private key and initial device identifier (IDevID) [1]), where it is stored in secure storage to prevent tampering or disclosure. This process includes generation of the credential (e.g., a private key and other information), signing of this credential (if applicable, depending on what onboarding protocol the device is designed to support), and transfer of the device bootstrapping information (e.g., a DPP URI or the device's IDevID) to the appropriate destination to ensure that it will be available for use during the network layer onboarding process. Following provisioning, the birth credential may be used for network-layer or application-layer onboarding. Table 2-1 lists the capabilities that may be demonstrated in this factory provisioning scenario.

Table 2-1 Scenario 0 Factory Provisioning Capabilities That May Be Demonstrated

Demo ID	Capability	Description
S0.C1	Birth Credential Generation and Storage	The device’s birth credentials are generated within or generated and provisioned into secure storage on the IoT device. The content and format of the credential are appropriate to the onboarding protocol (e.g., Wi-Fi Easy Connect [2] or BRSKI [3]) that the device is designed to support: • For BRSKI, the credential is a private key, a signed certificate (IDevID), a trust anchor for the manufacturer’s certificate authority (CA), and the location of a trusted manufacturer authorized signing authority (MASA). • For Wi-Fi Easy Connect, the credential is a private key and a public bootstrapping key.
S0.C2	Birth Credential Signing	The credential is signed by a trusted CA.
S0.C3	Bootstrapping Information Availability	The bootstrapping information required for onboarding the device is made available as needed. The format and content of the bootstrapping information depends on the onboarding protocol that the device is designed to support: • For BRSKI, the bootstrapping information is the certificate and ownership information that is sent to the MASA. • For Wi-Fi Easy Connect, the bootstrapping information is the Device Provisioning Protocol (DPP) uniform resource identifier (URI) (which contains the public key, and optionally other information such as device serial number).

2.2 Scenario 1: Trusted Network-Layer Onboarding

This scenario involves trusted network-layer onboarding of an authorized IoT device to a local network that is operated by the owner of the IoT device. The device is assumed to have been manufactured to support the type of network-layer onboarding protocol (e.g., Wi-Fi Easy Connect or BRSKI) that is being used by the local network. The device is also assumed to have been provisioned with its birth credential in a manner similar to that described in Scenario 0: Factory Provisioning, including transfer of the device’s bootstrapping information (e.g., its public key) to the operator of the local network to ensure that this information will be available to support authentication of the device during the initial phase of the trusted network-layer onboarding process. Onboarding is performed after the device has booted up and is placed in onboarding mode. Because the organization that is operating the local network is the owner of the IoT device, the device is authorized to onboard to the network and the network is authorized to onboard the device. In this scenario, after the identities of the device and the network are authenticated, a *network onboarding component*—a logical component authorized to onboard devices on behalf of the network—authenticates the device and provisions unique network credentials to the device over a secure channel. These network credentials are not just specific to the device; they are also specific to the local network. The device then uses these credentials to connect to the network. Table 2-2 lists the capabilities that may be demonstrated in this scenario.

Table 2-2 Scenario 1 Trusted Network-Layer Onboarding Capabilities That May Be Demonstrated

Demo ID	Capability	Description
S1.C1	Device Authentication	The onboarding mechanism authenticates the device's identity.
S1.C2	Device Authorization	The onboarding mechanism verifies that the device is authorized to onboard to the network.
S1.C3	Network Authentication	The device can verify the network's identity.
S1.C4	Network Authorization	The device can verify that the network is authorized to take control of it.
S1.C5	Secure Local Credentialing	The onboarding mechanism securely provisions local network credentials to the device.
S1.C6	Secure Storage	The local network credentials are provisioned to secure hardware-backed storage on the device.
S1.C7	Network Selection	The onboarding mechanism provides the IoT device with the identifier of the network to which the device should onboard.
S1.C8	Interoperability	The network-layer onboarding mechanism can onboard a minimum of two types of IoT devices (e.g., different device vendors and models).

2.3 Scenario 2: Trusted Application-Layer Onboarding

This scenario involves trusted application-layer onboarding that is performed automatically on an IoT device after the device 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, assuming the device has been designed and provisioned to support application-layer onboarding. As part of these steps, the device automatically mutually authenticates with a trusted application-layer onboarding service and establishes an encrypted connection to that service so the service can provision the device with application-layer credentials. The application-layer credentials could, for example, enable the device to securely connect to a trusted lifecycle management service to check for available updates or patches. For the application-layer onboarding mechanism to be trusted, it must establish an encrypted connection to the device without exposing any information that must be protected to ensure the confidentiality of that connection. Two types of application-layer onboarding are defined in NIST SP 1800-36B: *streamlined* and *independent*. Table 2-3 lists the capabilities that may be demonstrated in this scenario, including both types of application-layer onboarding.

Table 2-3 Scenario 2 Trusted Application-Layer Onboarding Capabilities That May Be Demonstrated

Demo ID	Capability	Description
S2.C1	Automatic Initiation of Streamlined Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been securely conveyed to the device during the network-layer onboarding process.
S2.C2	Automatic Initiation of Independent Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been pre-provisioned to the device by the device manufacturer or integrator (e.g., as part of an application that was installed on the device during the manufacturing process).
S2.C3	Trusted Application-Layer Onboarding	The device and a trusted application service can establish an encrypted connection without exposing any information that must be protected to ensure the confidentiality of the connection. They can then use that secure association to exchange application-layer information.

2.4 Scenario 3: Re-Onboarding a Device

This scenario involves re-onboarding an IoT device to a network after deleting its network credentials so that the device can be re-credentialed and reconnected. If the device also supports application-layer onboarding, application-layer onboarding should also be performed again after the device reconnects to the network. This scenario assumes that the device has been able to successfully demonstrate trusted network-layer onboarding as defined in Scenario 1: Trusted Network-Layer Onboarding. If application-layer re-onboarding is to be demonstrated as well, the scenario assumes that the device has also been able to successfully demonstrate at least one method of application-layer onboarding as defined in Scenario 2: Trusted Application-Layer Onboarding. Table 2-4 lists the capabilities that may be demonstrated in this scenario.

Table 2-4 Scenario 3 Re-Onboarding Capabilities That May Be Demonstrated

Demo ID	Capability	Description
S3.C1	Credential Deletion	The device’s network credential can be deleted.
S3.C2	De-Credentialed Device Cannot Connect	After the device’s network credential has been deleted, the device is not able to connect to or communicate on the network securely.
S3.C3	Re-Onboarding (network layer)	After the device’s network credential has been deleted, the network-layer onboarding mechanism can securely re-provision a network

Demo ID	Capability	Description
		credential to the device, which the device can then use to connect to the network securely.
S3.C4	Re-Onboarding (application layer)	After the device's network and application-layer credentials have been deleted and the device has been re-onboarded at the network layer and reconnected to the network, the device can again perform trusted application-layer onboarding.

2.5 Scenario 4: Ongoing Device Validation

This scenario involves ongoing validation of a device, not only as part of a trusted boot or attestation process prior to permitting the device to undergo network-layer onboarding, but also after the device has connected to the network. It may involve one or more security mechanisms that are designed to evaluate, validate, or respond to device trustworthiness using methods such as examining device behavior, ensuring device authenticity and integrity, and assigning the device to a specific network segment based on its conformance to policy criteria. Table 2-5 lists the capabilities that may be demonstrated in this scenario. None of these capabilities are integral to trusted network-layer onboarding; however, they may be used in conjunction with, or subsequent to, trusted network-layer onboarding to enhance device and network security.

Table 2-5 Scenario 4 Ongoing Device Validation Capabilities That May Be Demonstrated

Demo ID	Capability	Description
S4.C1	Device Attestation (initial)	The network-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.
S4.C2	Device Attestation (application layer)	The application-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.
S4.C3	Device Attestation (ongoing)	Successful device attestation is required prior to permitting the device to perform some operation (e.g., accessing a high-value resource).
S4.C4	Local Network Segmentation (initial)	Upon connection, the IoT device is assigned to some local network segment in accordance with policy, which may include an assessment of its security posture.
S4.C5	Behavioral Analysis	Device behavior is observed to determine whether the device meets the policy criteria required to be permitted to perform a given operation (e.g., to access a high-value resource or be placed on a given network segment).
S4.C6	Local Network Segmentation (ongoing)	The IoT device can be reassigned to a different network segment based on ongoing assessments of its conformance to policy criteria.
S4.C7	Periodic Device Reauthentication	After connection, the IoT device's identity is periodically reauthenticated in order to maintain network access.

Demo ID	Capability	Description
S4.C8	Periodic Device Reauthorization	After connection, the IoT device's authorization to access the network is periodically reconfirmed in order to maintain network access.

2.6 Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle

This scenario involves steps used to help establish and maintain the security posture of both the device's network credentials and the device itself. It includes the capability to download and validate the device's most recent firmware updates, securely integrate with a device communications intent enforcement mechanism (e.g., Manufacturer Usage Description (MUD) [4]), keep the device updated and patched, and establish and maintain the device's network credentials by provisioning X.509 certificates or DPP Connectors to the device and updating expired network credentials. Table 2-6 lists the capabilities that may be demonstrated in this scenario. None of these capabilities are integral to trusted network-layer onboarding; however, they may be used in conjunction with or subsequent to trusted network-layer onboarding to enhance device and network security.

Table 2-6 Scenario 5 Credential and Device Posture Establishment and Maintenance Capabilities That May Be Demonstrated

Demo ID	Capability	Description
S5.C1	Trusted Firmware Updates	The device can download the most recent firmware update and verify its signature before it is installed.
S5.C2	Credential Certificate Provisioning	The onboarding mechanism can interact with a certificate authority to sign a device's X.509 certificate and provision it onto the device.
S5.C3	Credential Update	The device's network credential can be updated after it expires.
S5.C4	Server Attestation	Successful server attestation is required prior to permitting the server to perform some operation on the device (e.g., prior to downloading and installing updates onto the device).
S5.C5	Secure Integration with MUD	The network-layer onboarding mechanism can convey necessary device communications intent information (e.g., the IoT device's MUD URL) to the network in encrypted form, thereby securely binding this information to the device and ensuring its confidentiality and integrity.
S5.C6	Lifecycle Management Establishment	The device has a lifecycle management service and can automatically establish a secure association with it after performing network-layer onboarding and connecting to the network.

3 Functional Demonstration Results

This section records the capabilities that were demonstrated for each of the builds.

3.1 Build 1 Demonstration Results

Table 3-1 lists the capabilities that were demonstrated by Build 1.

Table 3-1 Build 1 Capabilities Demonstrated

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 0: Factory Provisioning				
S0.C1	Birth Credential Generation and Storage	The device's birth credentials are generated within or generated and provisioned into secure storage on the IoT device. For Wi-Fi Easy Connect, the credential is a private key and a public bootstrapping key.	Yes	Public/private key-pair is generated within the SEALSQ VaultIC secure element.
S0.C2	Birth Credential Signing	The credential is signed by a trusted CA.	No	There is no requirement to support this capability in this build. Birth credentials for devices supporting Wi-Fi Easy Connect onboarding do not need to be signed.
S0.C3	Bootstrapping Information Availability	The bootstrapping information required for onboarding the device is made available as needed. For Wi-Fi Easy Connect, the bootstrapping information is the Device Provisioning Protocol (DPP) uniform resource identifier (URI) (which contains the public key, and optionally other information such as device serial number).	Yes	The device's DPP URI is generated using the public/private keypair that was generated in the device's secure element. This DPP URI is encoded in a QR code that is written to a Portable Network Graphics (PNG) file and may be transferred from a vendor cloud upon acquisition of the device.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 1: Trusted Network-Layer Onboarding				
S1.C1	Device Authentication	The onboarding mechanism authenticates the device's identity.	Yes	DPP performs device authentication.
S1.C2	Device Authorization	The onboarding mechanism verifies that the device is authorized to onboard to the network.	Yes	When the device's URI is found on the HPE cloud service, this verifies that the device is authorized to onboard to the network.
S1.C3	Network Authentication	The device can verify the network's identity.	No	This could be supported by providing the IoT device with the DPP URI of the network, but the Aruba User Experience Insight (UXI) sensor used in this build lacks the user interface needed to do so.
S1.C4	Network Authorization	The device can verify that the network is authorized to take control of it.	Yes	The network that possesses the device's public key is implicitly authorized to onboard the device by virtue of its knowledge of the device's public key. While this is not cryptographic, it does provide a certain level of assurance that the "wrong" network doesn't take control of the device.
S1.C5	Secure Local Credentialing	The onboarding mechanism securely provisions local network credentials to the device.	Yes	DPP provisions the device's network credentials over an encrypted channel.
S1.C6	Secure Storage	The local network credentials are provisioned to secure hardware-backed storage on the device.	No	The bootstrapping credentials are stored in a Trusted Platform Module (TPM) 2.0 hardware enclave, but the local network credentials are not
S1.C7	Network Selection	The onboarding mechanism provides	Yes	The network responds to device chirps.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		the IoT device with the identifier of the network to which the device should onboard.		
S1.C8	Interoperability	The network-layer onboarding mechanism can onboard a minimum of two types of IoT devices (e.g., different device vendors and models).	Yes	IoT devices from Build 2 were successfully onboarded in Build 1.
Scenario 2: Trusted Application-Layer Onboarding				
S2.C1	Automatic Initiation of Streamlined Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been securely conveyed to the device during the network-layer onboarding process.	No	Not supported in this build.
S2.C2	Automatic Initiation of Independent Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been	Yes	Once onboarded, the UXI sensor automatically initiates application-layer onboarding to the UXI application.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		pre-provisioned to the device by the device manufacturer or integrator (e.g., as part of an application that was installed on the device during the manufacturing process).		
S2.C3	Trusted Application- Layer Onboarding	The device and a trusted application service can establish an encrypted connection without exposing any information that must be protected to ensure the confidentiality of the connection. They can then use that secure association to exchange application-layer information.	Yes	Once onboarded, the UXI sensor establishes a secure connection with the UXI cloud, which provisions the sensor with its credentials for the UXI application. Later, the sensor uploads data to the UXI application securely.
Scenario 3: Re-Onboarding a Device				
S3.C1	Credential Deletion	The device's network credential can be deleted.	Yes	Factory reset and manual credential removal were leveraged.
S3.C2	De-Credentialed Device Cannot Connect	After the device's network credential has been deleted, the device is not able to connect to or communicate on the network securely.	Yes	Observed.
S3.C3	Re-Onboarding (network layer)	After the device's network credential has been deleted, the network-layer onboarding mechanism can security re-provision a network credential to the device, which the device can then use to	Yes	Observed.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		connect to the network securely.		
S3.C4	Re-Onboarding (application layer)	After the device's network and application-layer credentials have been deleted and the device has been re-onboarded at the network layer and re-connected to the network, the device can again perform trusted application-layer onboarding.	Yes	Observed.
Scenario 4: Ongoing Device Validation				
S4.C1	Device Attestation (initial)	The network-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C2	Device Attestation (application layer)	The application-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C3	Device Attestation (ongoing)	Successful device attestation is required prior to permitting the device to perform some operation (e.g., accessing a high-value resource).	No	Not supported in this build.
S4.C4	Local Network Segmentation (initial)	Upon connection, the IoT device is assigned to some local network segment in accordance with policy, which may	No	Not demonstrated in this phase.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		include an assessment of its security posture.		
S4.C5	Behavioral Analysis	Device behavior is observed to determine whether the device meets the policy criteria required to be permitted to perform a given operation (e.g., to access a high-value resource or be placed on a given network segment).	No	Not supported in this build.
S4.C6	Local Network Segmentation (ongoing)	The IoT device can be reassigned to a different network segment based on ongoing assessments of its conformance to policy criteria.	No	Not supported in this build.
S4.C7	Periodic Device Reauthentication	After connection, the IoT device's identity is periodically reauthenticated in order to maintain network access.	No	Not supported in this build.
S4.C8	Periodic Device Reauthorization	After connection, the IoT device's authorization to access the network is periodically reconfirmed in order to maintain network access.	No	Not supported in this build.
Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle				
S5.C1	Trusted Firmware Updates	The device can download the most recent firmware update and verify its signature before it is installed.	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S5.C2	Credential Certificate Provisioning	The onboarding mechanism can interact with a certificate authority to sign a device's X.509 certificate and provision it onto the device.	Yes	This capability has been successfully demonstrated with the SEALSQ INeS CA.
S5.C3	Credential Update	The device's network credential can be updated after it expires.	No	Not demonstrated in this phase.
S5.C4	Server Attestation	Successful server attestation is required prior to permitting the server to perform some operation on the device (e.g., prior to downloading and installing updates onto the device).	No	Not supported in this build.
S5.C5	Secure Integration with MUD	The network-layer onboarding mechanism can convey necessary device communications intent information (e.g., the IoT device's MUD URL) to the network in encrypted form, thereby securely binding this information to the device and ensuring its confidentiality and integrity.	No	Supported by DPP, but not demonstrated because Build 1 is not integrated with MUD or any other device communications intent enforcement mechanism.
S5.C6	Lifecycle Management Establishment	The device has a lifecycle management service and can automatically establish a secure association with it after performing network-layer onboarding and	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		connecting to the network.		

309 ## 3.2 Build 2 Demonstration Results

310 Table 3-2 lists the capabilities that were demonstrated by Build 2.

311 **Table 3-2 Build 2 Capabilities Demonstrated**

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 1: Trusted Network-Layer Onboarding				
S1.C1	Device Authentication	The onboarding mechanism authenticates the device's identity.	Yes	DPP performs device authentication.
S1.C2	Device Authorization	The onboarding mechanism verifies that the device is authorized to onboard to the network.	Yes	Only devices that have been added/approved by the administrator are onboarded. When the device's URI is found, the controller authorizes the device to join the network.
S1.C3	Network Authentication	The device can verify the network's identity.	No	This could be supported by providing the IoT device with the DPP URI of the network, but this is not currently implemented.
S1.C4	Network Authorization	The device can verify that the network is authorized to take control of it.	Yes	The network that possesses the device's public key is implicitly authorized to onboard the device by virtue of its knowledge of the device's public key. While this is not cryptographic, it does provide a certain level of assurance that the "wrong" network doesn't take control of the device.
S1.C5	Secure Local Credentialing	The onboarding mechanism securely provisions local	Yes	DPP provisions the device's network credentials over an encrypted channel.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		network credentials to the device.		
S1.C6	Secure Storage	The local network credentials are provisioned to secure hardware-backed storage on the device.	No	The IoT device does not have secure hardware-backed storage.
S1.C7	Network Selection	The onboarding mechanism provides the IoT device with the identifier of the network to which the device should onboard.	Yes	Network responds to device chirps.
S1.C8	Interoperability	The network-layer onboarding mechanism can onboard a minimum of two types of IoT devices (e.g., different device vendors and models).	Yes	Build 2 was able to onboard the IoT devices from Build 1.
		Scenario 2: Trusted Application-Layer Onboarding		
S2.C1	Automatic Initiation of Streamlined Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been securely conveyed to the device during the network-layer onboarding process.	Yes	This has been demonstrated with the OCF Iotivity [5] custom extension. Iotivity is an open-source software framework that implements OCF standards and enables seamless device-to-device connectivity.
S2.C2	Automatic Initiation of Independent	The device can automatically (i.e., with no manual intervention required) initiate	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
	Application-Layer Onboarding	trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been pre-provisioned to the device by the device manufacturer or integrator (e.g., as part of an application that was installed on the device during the manufacturing process).		
S2.C3	Trusted Application-Layer Onboarding	The device and a trusted application service can establish an encrypted connection without exposing any information that must be protected to ensure the confidentiality of the connection. They can then use that secure association to exchange application-layer information.	Yes	Once the device is onboarded to the network using DPP, the credentials for the application layer onboarding are sent over the secure channel and provisioned by the onboarding tool (OBT).
Scenario 3: Re-Onboarding a Device				
S3.C1	Credential Deletion	The device's network credential can be deleted.	Yes	Supports factory reset.
S3.C2	De-Credentialed Device Cannot Connect	After the device's network credential has been deleted, the device is not able to connect to or communicate on the network securely.	Yes	Observed.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S3.C3	Re-Onboarding (network layer)	After the device's network credential has been deleted, the network-layer onboarding mechanism can security re-provision a network credential to the device, which the device can then use to connect to the network securely.	Yes	Observed.
S3.C4	Re-Onboarding (application layer)	After the device's network and application-layer credentials have been deleted and the device has been re-onboarded at the network layer and re-connected to the network, the device can again perform trusted application-layer onboarding.	Yes	Observed.
Scenario 4: Ongoing Device Validation				
S4.C1	Device Attestation (initial)	The network-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C2	Device Attestation (application layer)	The application-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C3	Device Attestation (ongoing)	Successful device attestation is required prior to permitting the device to perform some operation (e.g.,	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		accessing a high-value resource).		
S4.C4	Local Network Segmentation (initial)	Upon connection, the IoT device is assigned to some local network segment in accordance with policy, which may include an assessment of its security posture.	Yes	When the device is connected to the network, the gateway places it in a restricted network segment based on policy.
S4.C5	Behavioral Analysis	Device behavior is observed to determine whether the device meets the policy criteria required to be permitted to perform a given operation (e.g., to access a high-value resource or be placed on a given network segment).	No	Not supported in this build.
S4.C6	Local Network Segmentation (ongoing)	The IoT device can be reassigned to a different network segment based on ongoing assessments of its conformance to policy criteria.	Yes	Device can be moved to new network segments programmatically. The policy to do this is not defined in this build.
S4.C7	Periodic Device Reauthentication	After connection, the IoT device's identity is periodically reauthenticated in order to maintain network access.	No	Not supported in this build.
S4.C8	Periodic Device Reauthorization	After connection, the IoT device's authorization to access the network is periodically reconfirmed in order to maintain network access.	No	Not supported in this build.
Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle				

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S5.C1	Trusted Firmware Updates	The device can download the most recent firmware update and verify its signature before it is installed.	No	Not supported in this build.
S5.C2	Credential Certificate Provisioning	The onboarding mechanism can interact with a certificate authority to sign a device's X.509 certificate and provision it onto the device.	No	Not supported in this build.
S5.C3	Credential Update	The device's network credential can be updated after it expires.	No	Not demonstrated in this phase.
S5.C4	Server Attestation	Successful server attestation is required prior to permitting the server to perform some operation on the device (e.g., prior to downloading and installing updates onto the device).	No	Not supported in this build.
S5.C5	Secure Integration with MUD	The network-layer onboarding mechanism can convey necessary device communications intent information (e.g., the IoT device's MUD URL) to the network in encrypted form, thereby securely binding this information to the device and ensuring its confidentiality and integrity.	No	Supported by DPP, but not demonstrated because Build 2 is not integrated with MUD or any other device communications intent enforcement mechanism.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S5.C6	Lifecycle Management Establishment	The device has a lifecycle management service and can automatically establish a secure association with it after performing network-layer onboarding and connecting to the network.	No	Not supported in this build.

312 ## 3.3 Build 3 Demonstration Results

313 Table 3-3 lists the capabilities that were demonstrated by Build 3.

314 **Table 3-3 Build 3 Capabilities Demonstrated**

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 1: Trusted Network-Layer Onboarding				
S1.C1	Device Authentication	The onboarding mechanism authenticates the device's identity.	Yes	The local domain registrar receives the voucher request.
S1.C2	Device Authorization	The onboarding mechanism verifies that the device is authorized to onboard to the network.	Yes	The registrar verifies that the device is from an authorized manufacturer.
S1.C3	Network Authentication	The device can verify the network's identity.	Yes	Demonstrated by the voucher.
S1.C4	Network Authorization	The device can verify that the network is authorized to take control of it.	Yes	The registrar examines the new voucher and passes it to the device for onboarding.
S1.C5	Secure Local Credentialing	The onboarding mechanism securely provisions local network credentials to the device.	Yes	A local device identifier (LDevID) (i.e., the device's network credential) [1] is provisioned to the device after the device authentication and authorization process.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S1.C6	Secure Storage	The local network credentials are provisioned to secure hardware-backed storage on the device.	No	Not demonstrated in this phase.
S1.C7	Network Selection	The onboarding mechanism provides the IoT device with the identifier of the network to which the device should onboard.	No	Not demonstrated in this build.
S1.C8	Interoperability	The network-layer onboarding mechanism can onboard a minimum of two types of IoT devices (e.g., different device vendors and models).	No	Supported by BRSKI, but not demonstrated in this build.
Scenario 2: Trusted Application-Layer Onboarding				
S2.C1	Automatic Initiation of Streamlined Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been securely conveyed to the device during the network-layer onboarding process.	No	Not supported in this build.
S2.C2	Automatic Initiation of Independent Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been pre-provisioned to the device by the device manufacturer or integrator (e.g., as part of an application that was installed on the device during the manufacturing process).		
S2.C3	Trusted Application-Layer Onboarding	The device and a trusted application service can establish an encrypted connection without exposing any information that must be protected to ensure the confidentiality of the connection. They can then use that secure association to exchange application-layer information.	No	Not supported in this build.
Scenario 3: Re-Onboarding a Device				
S3.C1	Credential Deletion	The device's network credential can be deleted.	Yes	Observed.
S3.C2	De-Credentialed Device Cannot Connect	After the device's network credential has been deleted, the device is not able to connect to or communicate on the network securely.	Yes	Observed.
S3.C3	Re-Onboarding (network-layer)	After the device's network credential has been deleted, the	Yes	Observed.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		network-layer onboarding mechanism can security re-provision a network credential to the device, which the device can then use to connect to the network securely.		
S3.C4	Re-Onboarding (application layer)	After the device's network credentials have been deleted and the device has been re-onboarded at the network layer and re-connected to the network, the device can perform application-layer onboarding automatically.	No	Not supported in this build.
Scenario 4: Ongoing Device Validation				
S4.C1	Device Attestation (initial)	The network-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C2	Device Attestation (application layer)	The application-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C3	Device Attestation (ongoing)	Successful device attestation is required prior to permitting the device to perform some operation (e.g., accessing a high-value resource).	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S4.C4	Local Network Segmentation (initial)	Upon connection, the IoT device is assigned to some local network segment in accordance with policy, which may include an assessment of its security posture.	No	Not supported in this build.
S4.C5	Behavioral Analysis	Device behavior is observed to determine whether the device meets the policy criteria required to be permitted to perform a given operation (e.g., to access a high-value resource or be placed on a given network segment).	No	Not supported in this build.
S4.C6	Local Network Segmentation (ongoing)	The IoT device can be reassigned to a different network segment based on ongoing assessments of its conformance to policy criteria.	No	Not supported in this build.
S4.C7	Periodic Device Reauthentication	After connection, the IoT device's identity is periodically reauthenticated in order to maintain network access.	No	Not supported in this build.
S4.C8	Periodic Device Reauthorization	After connection, the IoT device's authorization to access the network is periodically reconfirmed in order to maintain network access.	No	Not supported in this build.
Scenario 5: Establish and Maintain Credential and Device Security Posture Throughout the Lifecycle				
S5.C1	Trusted Firmware Updates	The device can download the most recent firmware update	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		and verify its signature before it is installed.		
S5.C2	Credential Certificate Provisioning	The onboarding mechanism can interact with a certificate authority to sign a device's X.509 certificate and provision it onto the device.	Yes	A vendor-installed X.509 certificate and a vendor's authorizing service use link-local connectivity to provision device credentials.
S5.C3	Credential Update	The device's network credential (e.g., its LDevID or X.509 certificate) can be updated after it expires.	No	Will be demonstrated in a future implementation of this build.
S5.C4	Server Attestation	Successful server attestation is required prior to permitting the server to perform some operation on the device (e.g., prior to downloading and installing updates onto the device).	No	Not supported in this build.
S5.C5	Secure Integration with MUD	The network-layer onboarding mechanism can convey necessary device communications intent information (e.g., the IoT device's MUD URL) to the network in encrypted form, thereby securely binding this information to the device and ensuring its confidentiality and integrity.	No	Supported by BRSKI, but not demonstrated because Build 3 is not integrated with MUD or any other device communications intent enforcement mechanism.
S5.C6	Lifecycle Management Establishment	The device has a lifecycle management service and can automatically establish a secure association	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		with it after performing network-layer onboarding and connecting to the network.		

3.4 Build 4 Demonstration Results

Table 3-4 lists the capabilities that were demonstrated by Build 4.

Table 3-4 Build 4 Capabilities Demonstrated

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 1: Trusted Network-Layer Onboarding				
S1.C1	Device Authentication	The onboarding mechanism authenticates the device's identity.	No	The build performs trusted application-layer onboarding only.
S1.C2	Device Authorization	The onboarding mechanism verifies that the device is authorized to onboard to the network.	No	The build performs trusted application-layer onboarding only.
S1.C3	Network Authentication	The device can verify the network's identity.	No	The build performs trusted application-layer onboarding only.
S1.C4	Network Authorization	The device can verify that the network is authorized to take control of it.	No	The build performs trusted application-layer onboarding only.
S1.C5	Secure Local Credentialing	The onboarding mechanism securely provisions local network credentials to the device.	No	The build performs trusted application-layer onboarding only.
S1.C6	Secure Storage	The local network credentials are provisioned to secure hardware-backed storage on the device.	Yes	The local network credentials are stored in the Silicon Labs Secure Vault on the Thunderboard.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S1.C7	Network Selection	The onboarding mechanism provides the IoT device with the identifier of the network to which the device should onboard.	No	The device generates a pre-shared key that is manually entered in the OpenThread Border Router [6].
S1.C8	Interoperability	The network-layer onboarding mechanism can onboard a minimum of two types of IoT devices (e.g., different device vendors and models).	No	Not supported in this build.
Scenario 2: Trusted Application-Layer Onboarding				
S2.C1	Automatic Initiation of Streamlined Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been securely conveyed to the device during the network-layer onboarding process.	No	Not supported in this build.
S2.C2	Automatic Initiation of Independent Application-	The device can automatically (i.e., with no manual intervention required) initiate	Yes	Trusted application-layer onboarding using Kudelski keySTREAM is configured to proceed automatically pending

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
	Layer Onboarding	trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been pre-provisioned to the device by the device manufacturer or integrator (e.g., as part of an application that was installed on the device during the manufacturing process).		confirmation from a user (through the press of a button).
S2.C3	Trusted Application-Layer Onboarding	The device and a trusted application service can establish an encrypted connection without exposing any information that must be protected to ensure the confidentiality of the connection. They can then use that secure association to exchange application-layer information.	Yes	Application Layer Onboarding via Kudelski keySTREAM GUI / AWS IoT Core and through the Silicon Labs Simplicity Studio Device Console
Scenario 3: Re-Onboarding a Device				
S3.C1	Credential Deletion	The device's network credential can be deleted.	Yes	The device can be removed from the network via the Open Thread Border Router

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
				GUI and cannot rejoin without entering a new pre-shared key.
S3.C2	De-Credentialed Device Cannot Connect	After the device's network credential has been deleted, the device is not able to connect to or communicate on the network securely.	Yes	Observed.
S3.C3	Re-Onboarding (network layer)	After the device's network credential has been deleted, the network-layer onboarding mechanism can security re-provision a network credential to the device, which the device can then use to connect to the network securely.	Yes	Observed.
S3.C4	Re-Onboarding (application layer)	After the device's network and application-layer credentials have been deleted and the device has been re-onboarded at the network layer and re-connected to the network, the device can again perform trusted application-layer onboarding.	Yes	Observed.
Scenario 4: Ongoing Device Validation				
S4.C1	Device Attestation (initial)	The network-layer onboarding mechanism requires successful device attestation prior to permitting the	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		device to be onboarded.		
S4.C2	Device Attestation (application layer)	The application-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C3	Device Attestation (ongoing)	Successful device attestation is required prior to permitting the device to perform some operation (e.g., accessing a high-value resource).	No	Not supported in this build.
S4.C4	Local Network Segmentation (initial)	Upon connection, the IoT device is assigned to some local network segment in accordance with policy, which may include an assessment of its security posture.	No	Not supported in this build.
S4.C5	Behavioral Analysis	Device behavior is observed to determine whether the device meets the policy criteria required to be permitted to perform a given operation (e.g., to access a high-value resource or be placed on a given network segment).	No	Not supported in this build.
S4.C6	Local Network Segmentation (ongoing)	The IoT device can be reassigned to a different network	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		segment based on ongoing assessments of its conformance to policy criteria.		
S4.C7	Periodic Device Reauthentication	After connection, the IoT device's identity is periodically reauthenticated in order to maintain network access.	No	Not supported in this build.
S4.C8	Periodic Device Reauthorization	After connection, the IoT device's authorization to access the network is periodically reconfirmed in order to maintain network access.	No	Not supported in this build.
Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle				
S5.C1	Trusted Firmware Updates	The device can download the most recent firmware update and verify its signature before it is installed.	No	Not supported in this build.
S5.C2	Credential Certificate Provisioning	The onboarding mechanism can interact with a certificate authority to sign a device's X.509 certificate and provision it onto the device.	No	Not supported in this build.
S5.C3	Credential Update	The device's network credential can be updated after it expires.	No	Not supported in this build.
S5.C4	Server Attestation	Successful server attestation is required prior to permitting the	No	Not supported in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		server to perform some operation on the device (e.g., prior to downloading and installing updates onto the device).		
S5.C5	Secure Integration with MUD	The network-layer onboarding mechanism can convey necessary device communications intent information (e.g., the IoT device's MUD URL) to the network in encrypted form, thereby securely binding this information to the device and ensuring its confidentiality and integrity.	No	Not supported in this build.
S5.C6	Lifecycle Management Establishment	The device has a lifecycle management service and can automatically establish a secure association with it after performing network-layer onboarding and connecting to the network.	No	Not supported in this build.

3.5 Build 5 Demonstration Results

Table 3-5 lists the capabilities that were demonstrated by Build 5.

Table 3-5 Build 5 Capabilities Demonstrated

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 0: Factory Provisioning				
S0.C1	Birth Credential Generation and Storage	The device's birth credentials are generated within or generated and provisioned into secure storage on the IoT device. For BRSKI, the credential is an IDevID certificate.	Yes	Supporting public/private keypair is generated within the secure element, and signed IDevID certificate is placed into the secure element.
S0.C2	Birth Credential Signing	The credential is signed by a trusted CA.	Yes	The IDevID certificate is signed by the Build 5 Manufacturer Provisioning Root (MPR).
S0.C3	Bootstrapping Information Availability	The bootstrapping information required for onboarding the device is made available as needed. For BRSKI, the bootstrapping information is the IDevID certificate provisioned into the device's secure element.	Yes	The device's IDevID certificate is generated using the public/private keypair that was generated in the device's secure element. This IDevID certificate is presented to verify the device's identity during network-layer onboarding.
Scenario 1: Trusted Network-Layer Onboarding				
S1.C1	Device Authentication	The onboarding mechanism authenticates the device's identity.	Yes	The device is authenticated using its provisioned IDevID.
S1.C2	Device Authorization	The onboarding mechanism verifies that the device is authorized to onboard to the network.	Yes	The device is implicitly granted authorization during the onboarding process within the registrar implementation. However, this authorization is contingent upon the device satisfying the policy

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
				requirements for onboarding.
S1.C3	Network Authentication	The device can verify the network's identity.	Yes	Demonstrated by the voucher.
S1.C4	Network Authorization	The device can verify that the network is authorized to take control of it.	Yes	The device authenticates to the network using EAP-TLS. The registrar gets a voucher from the MASA verifying that the network is authorized to onboard the device and it passes this voucher to the device so the device can verify that the network is authorized to onboard it.
S1.C5	Secure Local Credentialing	The onboarding mechanism securely provisions local network credentials to the device.	Yes	A local device identifier (LDevID) (i.e., the device's network credential) [1] is provisioned to the device as the culmination of the network-layer onboarding process.
S1.C6	Secure Storage	The local network credentials are provisioned to secure hardware-backed storage on the device.	No	The IDevID (birth credential) keys are generated with a TPM secure element. The EAP-TLS negotiation is configured to use keys from the secure element. The local network credentials (LDevID) are not scored in secure storage.
S1.C7	Network Selection	The onboarding mechanism provides the IoT device with the identifier of the network to which the device should onboard.	Yes	The identifier of the network is passed back in the common name field of the LDevID X.509 certificate.
S1.C8	Interoperability	The network-layer onboarding mechanism can onboard a minimum of two types of IoT devices (e.g., different device vendors and models).	Yes	Supported by BRSKI over IEEE 802.11 [7], but not demonstrated in this build.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
Scenario 2: Trusted Application-Layer Onboarding				
S2.C1	Automatic Initiation of Streamlined Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been securely conveyed to the device during the network-layer onboarding process.	No	Not supported in this build
S2.C2	Automatic Initiation of Independent Application-Layer Onboarding	The device can automatically (i.e., with no manual intervention required) initiate trusted application-layer onboarding after performing network-layer onboarding and connecting to the network. In this case, the application-layer onboarding bootstrapping information has been pre-provisioned to the device by the device manufacturer or integrator (e.g., as part of an application that was installed on the device during the manufacturing process).	Yes	The pledge can use its IDevID and the private key in the secure element to automatically establish a TLS connection to an application server using OpenSSL s_client. The address of the application server has been pre-provisioned to the device by the manufacturer.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S2.C3	Trusted Application-Layer Onboarding	The device and a trusted application service can establish an encrypted connection without exposing any information that must be protected to ensure the confidentiality of the connection. They can then use that secure association to exchange application-layer information.	Yes	The pledge can use its IDevID and the private key in the secure element to automatically establish a TLS connection to an application server using OpenSSL s_client. The address of the application server has been pre-provisioned to the device by the manufacturer.
Scenario 3: Re-Onboarding a Device				
S3.C1	Credential Deletion	The device's network credential can be deleted.	Yes	The device is removed from Radius server by revoking its voucher.
S3.C2	De-Credentialed Device Cannot Connect	After the device's network credential has been deleted, the device is not able to connect to or communicate on the network securely.	Yes	If credential is removed from the registrar/radius server, the device will not connect. Certificate revocation through CRL is also implemented.
S3.C3	Re-Onboarding (network-layer)	After the device's network credential has been deleted, the network-layer onboarding mechanism can securely re-provision a network credential to the device, which the device can then use to connect to the network securely.	Yes	Upon a voucher being revoked, the LDevID is invalidated. The pledge can then perform the onboarding process again with a newly generated LDevID.
S3.C4	Re-Onboarding (application layer)	After the device's network credentials have been deleted and the device has been re-onboarded at the	Yes	After re-establishing a network connection, application onboarding happens automatically.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		network layer and re-connected to the network, the device can perform application-layer onboarding automatically.		
		Scenario 4: Ongoing Device Validation		
S4.C1	Device Attestation (initial)	The network-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C2	Device Attestation (application layer)	The application-layer onboarding mechanism requires successful device attestation prior to permitting the device to be onboarded.	No	Not supported in this build.
S4.C3	Device Attestation (ongoing)	Successful device attestation is required prior to permitting the device to perform some operation (e.g., accessing a high-value resource).	No	Not supported in this build.
S4.C4	Local Network Segmentation (initial)	Upon connection, the IoT device is assigned to some local network segment in accordance with policy, which may include an assessment of its security posture.	No	Not supported in this build.
S4.C5	Behavioral Analysis	Device behavior is observed to determine whether the device meets the policy criteria required to be permitted to perform a given operation (e.g., to access a high-value	Yes	Real time network events are propagated from the gateway(s) to the policy engine. When suspicious behavior is identified (e.g., contact denylisted IP address) device network access is revoked.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
		resource or be placed on a given network segment).		
S4.C6	Local Network Segmentation (ongoing)	The IoT device can be reassigned to a different network segment based on ongoing assessments of its conformance to policy criteria.	No	Not supported in this build.
S4.C7	Periodic Device Reauthentication	After connection, the IoT device's identity is periodically reauthenticated in order to maintain network access.	No	Not supported in this build.
S4.C8	Periodic Device Reauthorization	After connection, the IoT device's authorization to access the network is periodically reconfirmed in order to maintain network access.	Yes	The continuous assurance policy is checked periodically, every 30 seconds in the demo. The policy sets the requirements for a device to be authorized to have access to the network. If a device fails this check, its voucher is revoked, invalidating the device's LDevID.
Scenario 5: Establish and Maintain Credential and Device Security Posture Throughout the Lifecycle				
S5.C1	Trusted Firmware Updates	The device can download the most recent firmware update and verify its signature before it is installed.	No	Not supported in this build.
S5.C2	Credential Certificate Provisioning	The onboarding mechanism can interact with a certificate authority to sign a device's X.509 certificate and provision it onto the device.	Yes	In the BRSKI flows, the onboarding process results in an LDevID (X.509) certificate being provisioned on the device, after the trustworthiness checks have been completed. This LDevID certificate is signed by the Domain CA.

Demo ID	Capability	Description	Demonstrated?	Explanation/Notes
S5.C3	Credential Update	The device's network credential (e.g., its LDevID or X.509 certificate) can be updated after it expires.	Yes	Device will automatically generate a new LDevID and re-onboard if LDevID expires.
S5.C4	Server Attestation	Successful server attestation is required prior to permitting the server to perform some operation on the device (e.g., prior to downloading and installing updates onto the device).	No	Not supported in this build.
S5.C5	Secure Integration with MUD	The network-layer onboarding mechanism can convey necessary device communications intent information (e.g., the IoT device's MUD URL) to the network in encrypted form, thereby securely binding this information to the device and ensuring its confidentiality and integrity.	Yes	The continuous assurance policy engine sporadically resolves the MUD document of each unique connected device using all information available. In this build we use the D3DB method of resolution, which resolves using chained verifiable credentials; specifically, the MUD document is bound to the device ID using a simulated managed firmware service. This provides a verifiable credential binding a device identifier (IDevID) to a full MUD document.
S5.C6	Lifecycle Management Establishment	The device has a lifecycle management service and can automatically establish a secure association with it after performing network-layer onboarding and connecting to the network.	No	Not supported in this build.

Appendix A References

[1] *IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity*, IEEE Std 802.1AR-2018 (Revision of IEEE Std 802.1AR-2009), 2 Aug. 2018, 73 pp. Available: https://ieeexplore.ieee.org/document/8423794

[2] Wi-Fi Alliance, *Wi-Fi Easy Connect™ Specification Version 3.0*, 2022. Available: https://www.wi-fi.org/system/files/Wi-Fi_Easy_Connect_Specification_v3.0.pdf

[3] M. Pritikin, M. Richardson, T.T.E. Eckert, M.H. Behringer, and K.W. Watsen, *Bootstrapping Remote Secure Key Infrastructure (BRSKI)*, IETF Request for Comments (RFC) 8995, October 2021. Available: https://datatracker.ietf.org/doc/rfc8995/

[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

[5] Open Connectivity Foundation (OCF) Iotivity: https://iotivity.org/

[6] Thread 1.1.1 Specification, February 13, 2017.

[7] O. Friel, E. Lear, M. Pritikin, and M. Richardson, *BRSKI over IEEE 802.11*, IETF Internet-Draft (Individual), July 2018. Available: https://datatracker.ietf.org/doc/draft-friel-brski-over-802dot11/01/