NIST SPECIAL PUBLICATION 1800-36E

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

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume E:
Risk and Compliance Management

Michael Fagan
Jeffrey Marron
Paul Watrobski
Murugiah Souppaya
National Cybersecurity Center of Excellence
Information Technology Laboratory

Susan Symington
The MITRE Corporation
McLean, Virginia

Dan Harkins
Aruba, a Hewlett Packard Enterprise Company
San Jose, California

Steve Clark
SEALSQ, a Subsidiary of WISeKey
Geneva, Switzerland

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

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

William Barker
Dakota Consulting
Largo, Maryland

Nick Allott
Ashley Setter
NquiringMinds,
Southampton, United Kingdom

Brecht Wyseur
Kudelsky IoT
Cheseaux-sur-Lausanne, Switzerland

Mike Dow
Steve Egerter
Silicon Labs, Austin, Texas

Michael Richardson
Sandelman Software Works,
Ontario, Canada

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 1800-36E, Natl. Inst. Stand. Technol. Spec. Publ. 1800-36E, 22 pages, May 2024, CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback on the mappings included in this volume. Do you find the mappings that we have provided in this document helpful to you as you try to achieve your cybersecurity goals? Could the mappings that we have provided be improved, either in terms of their content or format? Are there additional standards, best practices, or other guidance documents that you would like us to map to and from trusted IoT device network-layer onboarding and lifecycle management capabilities? Are there additional use cases for these mappings that we should consider in the future? 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

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

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
Danny Jump	Aruba, a Hewlett Packard Enterprise company

Name	Organization
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
Todd Nuzum	NXP Semiconductors
Nicusor Penisoara	NXP Semiconductors
Laurentiu Tudor	NXP Semiconductors
Pedro Fuentes	SEALSQ, a subsidiary of WISeKey

Name	Organization
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	Foundries.io	Open Connectivity Foundation (OCF)
CableLabs	Kudelski IoT	Sandelman Software Works
Cisco	NquiringMinds	SEALSQ, a subsidiary of WISeKey
	NXP Semiconductors	Silicon Labs

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

In this project, the National Cybersecurity Center of Excellence (NCCoE) applies 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 discusses risks addressed by the trusted IoT device network-layer onboarding and lifecycle management reference design. It also maps between cybersecurity functionality provided by logical components of the reference design and Subcategories in the NIST Cybersecurity Framework (CSF) and controls in NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*. (Note: The reference design is described in detail in NIST SP 1800-36B, Section 4.)

Mappings are also provided between cybersecurity functionality provided by specific network-layer onboarding protocols (e.g., Wi-Fi Easy Connect and Bootstrapping Remote Secure Key Infrastructure [BRSKI]) and those same Subcategories and controls, as well as between cybersecurity functionality provided by builds of the reference design that have been implemented as part of this project and those same Subcategories and controls. (Note: the composition of the builds is described in detail in the appendices of NIST SP 1800-36B.)

None of the mappings we provide is intended to be exhaustive; the mappings focus on the strongest relationships involving each reference design cybersecurity function in order to help organizations prioritize their work. The mappings help users understand how trusted IoT device network-layer onboarding and lifecycle management can help them achieve their cybersecurity goals in terms of CSF Subcategories and SP 800-53 controls. The mappings also help users understand how they can implement trusted onboarding and lifecycle management by identifying how trusted onboarding functionality is supported by the user's existing implementations of CSF Subcategories and SP 800-53 controls.

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 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
- 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 best practices **(you are here)**

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 Risks Addressed by Trusted Network-Layer Onboarding and Lifecycle Management

Historically, IoT devices have not tended to be onboarded to networks in a trusted manner. This has left networks open to the threat of having unauthorized devices connect to them. It has also left devices open to the threat of being onboarded to networks that are not authorized to control them.

2.1 Risks to the Network

Unauthorized devices that are able to connect to a network pose many risks to that network. They may be able to send and receive data on that network, scan the network for vulnerabilities, eavesdrop on the communications of other devices, and attack other connected devices to exfiltrate or modify their data or to compromise those devices and co-opt them into service to launch distributed denial of service (DDoS) attacks.

2.1.1 Risks to the Network Due to Device Limitations

Many IoT devices are manufactured to be as inexpensive as possible, which sometimes means that the devices are not equipped with secure storage, cryptographic modules, unique authoritative birth credentials, or other features needed to enable the devices to be identified and authenticated. This can make it impossible for a network to determine if a device attempting to connect to it is the intended device. Lack of these features can also make it impossible to protect the confidentiality of a device's network credentials, both during the provisioning process and after the credentials have been installed on the device.

2.1.2 Risks to the Network Due to Use of Shared Network Credentials

If a network uses a single network password that is shared among all devices rather than providing each device with a unique network credential, the network will be vulnerable to having unauthorized devices connect to it if the shared network password falls into the wrong hands, which can happen relatively

easily. It also means that the network will permit devices to connect to it simply because a device presents the correct shared password, regardless of the device's type or identity, or whether it has any legitimate reason to connect to the network.

2.1.3 Risks to the Network Due to Insecure Network Credential Provisioning

If devices are manually provisioned with their network credentials, the provisioning process is error-prone, cumbersome, and vulnerable to having the device's network credentials disclosed. If the devices are provisioned automatically over Wi-Fi or some other interface that does not use an encrypted channel, the credentials are also vulnerable to unauthorized disclosure. If the network credentials are not provisioned in a trusted manner, the credentials are vulnerable to disclosure not only the first time the device is onboarded to the network, but every time it is onboarded, which may occur many times during the device lifecycle. For example, the device may need to be re-onboarded periodically to change its credentials in accordance with security policy, or it may need to be re-onboarded due to a security breach, hardware repair, security update, or other reasons. Any insecure features of the onboarding process, therefore, will render the device and network vulnerable every time the device is onboarded.

2.1.4 Risks to the Network Due to Supply Chain Attacks

If a device is compromised while in the supply chain or at some other point prior to being onboarded, then even though the device may be onboarded in a trusted manner, it may still pose a threat to the network, its data, and all devices connected to it. If, on the other hand, the trusted network-layer onboarding mechanism is integrated with a device attestation or supply chain management service that is capable of evaluating the integrity and provenance of the device and detecting that it has been compromised or may have been tampered with, the trusted network-layer onboarding mechanism could prevent such a compromised device from being onboarded and connected to the network.

2.2 Risks to the Device

Although it is relatively easy for one network to masquerade as another, IoT devices often do not authenticate the identity of the networks to which they allow themselves to be onboarded and connected. Devices may be unwittingly tricked into onboarding and connecting to imposter networks that are not authorized to onboard them. This makes those devices vulnerable to being taken control of by those unauthorized networks and thereby prevented from connecting to and providing their intended function on their authorized network.

2.3 Risks to Secure Lifecycle Management

Even if a device is authorized to connect to a network and the network is authorized to control the device, if the device has not been onboarded in a trusted manner, then other security-related operations that are performed after the device has connected to the network may not have as secure a foundation as they would if the device had been onboarded in a trusted manner. For example, if device communications intent enforcement is performed but the integrity and confidentiality of the communicated device intent information was not protected (as it would be by a trusted network-layer onboarding mechanism), then trust in the device communications intent enforcement mechanism may not be as robust as it could have been. Similarly, if application-layer onboarding is performed after the

device connects, but the information needed to bootstrap the application-layer onboarding process did not have its integrity and confidentiality protected (as it would be by a trusted network-layer onboarding mechanism), then trust in the application-layer onboarding mechanism may not be as robust as it could have been. Lack of trust in the application-layer onboarding mechanism may, in turn, undermine trust in the device lifecycle management or other application-layer service that is invoked as part of the application-layer onboarding process.

2.4 Limitations and Dependencies of Trusted Onboarding

While implementing trusted IoT device network-layer onboarding and lifecycle management addresses many risks, it also has limitations. Use of trusted network-layer onboarding is designed to enable IoT devices to be provisioned with unique local network credentials in a manner that preserves credential confidentiality. As part of the trusted network-layer onboarding process, the device and the network may mutually authenticate one another, thereby protecting the network from having unauthorized devices connect to it and the device from being taken over by an unauthorized network. However, if the network also enables devices that do not support the trusted network-layer onboarding solution to be provisioned with network credentials and connect to it using a different (untrusted) onboarding solution, the network and all devices on it will still be at risk from IoT devices that have been onboarded using untrusted mechanisms, and the devices that are onboarded using untrusted mechanisms will still be at risk of being taken over by networks that are not authorized to control them.

The trusted network-layer onboarding solution leverages the device's unique, authoritative *birth credentials*, which are provisioned to the device by the device manufacturer and must consist, at a minimum, of a unique device identity and a secret. The trustworthiness of the network-layer onboarding process and the network credentials that it provisions to the device depends on the uniqueness, integrity, and confidentiality of the device's birth credentials which, in many cases, depend on the device's hardware root of trust. If the manufacturer does not ensure that the device's credentials are unique, the identity of the device cannot be definitively authenticated. If the manufacturer is not able to maintain the confidentiality of the secret that is part of the device credentials, the trustworthiness of the device authentication process will be undermined, and the channel over which the device's credentials are provisioned will be vulnerable to eavesdropping.

The trusted network-layer onboarding solution depends upon the trustworthiness of the device's secure storage to ensure the confidentiality of the device and network credentials. If the device's secure storage is vulnerable, the trustworthiness of the network-layer onboarding process and the confidentiality of the device's network credentials will be compromised. If the secure storage in which the device's network credentials are stored is vulnerable, the network will be at risk of having unauthorized devices attach to it.

If the trusted network-layer onboarding mechanism is integrated with additional security capabilities such as device attestation, device communications intent enforcement, application-layer onboarding, and device lifecycle management, it can further increase trust in both the IoT device and, by extension, the network to which the device connects, assuming that these additional security capabilities themselves are secure and robust. If these security capabilities are not implemented correctly, then integrating with them is of no additional value and in fact may provide a false sense of security.

3 Mapping Use Cases, Approach, and Terminology

A *mapping* indicates that one concept is related to another concept. The remainder of this volume describes the mappings between trusted IoT device network-layer onboarding and lifecycle management cybersecurity functions and the security characteristics enumerated in relevant cybersecurity documents.

For this mapping, we have used the supportive relationship mapping style as defined in Section 4.2 of draft NIST Internal Report (IR) 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings* [1].

Each set of mappings involves one of the following types of trusted IoT device network-layer onboarding and lifecycle management cybersecurity functions:

- Cybersecurity functions performed by the reference design's logical components (see NIST SP 1800-36B Section 4)
- Cybersecurity functions provided by specific network-layer onboarding protocols (e.g., Wi-Fi Easy Connect and BRSKI)
- Cybersecurity functions provided by builds of the reference design that have been implemented as part of this project

Each of the cybersecurity functions is mapped to the security characteristics concepts found in the following widely used cybersecurity guidance documents:

- Subcategories from the NIST Cybersecurity Framework (CSF) 1.1 [2] which are also mapped to *The NIST Cybersecurity Framework 2.0 (CSF 2.0)* [3]. The CSF identifies enterprise-level security outcomes. Stakeholders have identified these outcomes as helpful for managing cybersecurity risk, but organizations adopting the CSF need to determine how to achieve the outcomes. Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [4], made the CSF mandatory for federal government agencies, and other government agencies and sectors have also made the CSF mandatory.
- Security controls from NIST SP 800-53r5 (*Security and Privacy Controls for Information Systems and Organizations*) [5]. NIST SP 800-53 identifies security controls that apply to systems on which those enterprises are reliant. Which SP 800-53 controls need to be employed depends on system functions and a risk assessment of the perceived impact of loss of system functionality or exposure of information from the system to unauthorized entities. In the case of systems owned by or operated on behalf of federal government enterprises, the risk assessment and applicable SP 800-53 controls are mandated under the Federal Information Security Modernization Act (FISMA) [6]. Many other governments and private sector organizations voluntarily employ the Risk Management Framework [7] and associated SP 800-53 controls.

3.1 Use Cases

All of the elements in these mappings—the trusted IoT device network-layer onboarding and lifecycle management cybersecurity functions, cybersecurity functions provided by specific network-layer onboarding protocols, cybersecurity functions provided by specific builds, CSF Subcategories, and SP 800-53 controls—are concepts involving ways to reduce cybersecurity risk.

There are two primary use cases for this mapping. They are not intended to be comprehensive, but rather to capture the strongest relationships involving the trusted IoT device network-layer onboarding and lifecycle management cybersecurity functions.

1. **Why should organizations implement trusted IoT device network-layer onboarding and lifecycle management?** This use case identifies how implementing trusted IoT device network-layer onboarding and lifecycle management can support organizations with achieving CSF Subcategories and SP 800-53 controls. This helps communicate to an organization's chief information security officer, security team, and senior management that expending resources to implement trusted IoT device network-layer onboarding and lifecycle management can also aid in fulfilling other security requirements.

2. **How can organizations implement trusted IoT device network-layer onboarding and lifecycle management?** This use case identifies how an organization's existing implementations of CSF Subcategories and SP 800-53 controls can help support a trusted IoT device network-layer onboarding and lifecycle management implementation. An organization wanting to implement trusted IoT device network-layer onboarding and lifecycle management might first assess its current security capabilities so that it can plan how to add missing capabilities and enhance existing capabilities. Organizations can leverage their existing security investments and prioritize future security technology deployment to address the gaps.

These mappings are intended to be used by any organization that is interested in implementing trusted IoT device network-layer onboarding and lifecycle management or that has begun or completed an implementation.

3.2 Mapping Producers

The NCCoE trusted IoT device network-layer onboarding and lifecycle management project team performed the mappings between the cybersecurity functions performed by the reference design's logical components (see NIST SP 1800 36B Section 4) and the security characteristics in the cybersecurity documents. They also performed the mappings between the cybersecurity functions performed by the specific network-layer onboarding protocols (i.e., Wi-Fi Easy Connect and BRSKI) and the security characteristics in the cybersecurity documents. These mappings were performed with input and feedback from the collaborators who have contributed technology to the builds of the reference design. Collaborators for each build, in conjunction with the NCCoE trusted IoT device network-layer onboarding and lifecycle management project team, performed the mappings between the cybersecurity functions provided by their contributed technologies in each build and the security characteristics in the cybersecurity documents.

3.3 Mapping Approach

In addition to performing general mappings between the reference design's cybersecurity functions and various sets of security characteristics, as well as between specific network-layer onboarding protocol cybersecurity functions and various sets of security characteristics, the NCCoE asked the collaborators for each build to indicate the mapping between the cybersecurity functions their technology components provide in that build and the sets of security characteristics.

Using the logical components in the reference design as the organizing principle for the initial mapping of cybersecurity functions to security characteristics and then providing onboarding protocol-specific mappings was intended to make it easier for collaborators to map their build-specific technology contributions. Using this approach, the build-specific technology mappings are instantiations of the project's general reference design and protocol-specific mappings for each document.

3.3.1 Mapping Terminology

In this publication, we use the following relationship types from NIST IR 8477 [1] to describe how the functions in our reference design are related to the NIST reference documents. Note that the *Supports* relationship applies only to use case 1 in Section 3.1 and the *Is Supported By* relationship applies only to use case 2.

- **Supports:** Trusted IoT device network-layer onboarding and lifecycle management function X *supports* security control/Subcategory/capability/requirement Y when X can be applied alone or in combination with one or more other functions to achieve Y in whole or in part.
- **Is Supported By:** Trusted IoT device network-layer onboarding and lifecycle management function X is *supported by* security control/Subcategory/capability/requirement Y when Y can be applied alone or in combination with one or more other security controls/Subcategories/capabilities/requirements to achieve X in whole or in part.

Each *Supports* and *Is Supported By* relationship has one of the following properties assigned to it:

- **Example of:** The supporting concept X is one way (*an example*) of achieving the supported concept Y in whole or in part. However, Y could also be achieved without applying X.
- **Integral to:** The supporting concept X is *integral to* and a component of the supported concept Y. X must be applied as part of achieving Y.
- **Precedes:** The supporting concept X *precedes* the supported concept Y when X must be achieved before applying Y. In other words, X is a prerequisite for Y.

When determining whether a reference design function's support for a given CSF Subcategory or SP 800-53 control is integral to that support versus an example of that support, we do not consider how that function may in general be used to support the Subcategory, control, capability, or requirement. Rather, we consider only how that function is intended to support that Subcategory, control, capability, or requirement within the context of our reference design.

Also, when determining whether a function is supported by a CSF Subcategory, SP 800-53 control, capability, etc. with the relationship property of *precedes*, we do not consider whether it is possible to apply the function without first achieving the Subcategory, control, capability, or requirement. Rather, we consider whether, according to our reference design, the Subcategory, control, capability, or requirement is to be achieved prior to applying that function.

3.3.2 Mapping Process

The process that the NCCoE used to create the mapping from the logical components of the reference design to the security characteristics of a given document was as follows:

1. Create a table that lists each of the logical components of the reference design in column 1.

2. Describe each logical component's cybersecurity function in column 2.
3. Map each cybersecurity function to each of the security characteristics in the document to which the function is most strongly related, and list each of these security characteristics on different sub-rows within column 3. Begin each security characteristic entry with an underlined keyword that describes the mapping's relationship type (i.e., *Supports*, *Is Supported By*). After the keyword indicating the relationship type, put in parentheses the underlined keyword describing the relationship's property (i.e., *Example of*, *Integral to*, or *Precedes*).
4. In the fourth column, provide a brief explanation of why that relationship type and property apply to the mapping.
5. After completing the mapping table entries as described above for all the logical components in the reference design, examine the mapping in the other direction, i.e., starting with the security characteristics listed in the document and considering whether they have a relationship to the logical components' cybersecurity functions in the reference design. In other words, step through each of the security characteristics in the document and determine if there is some logical component in the reference design that has a strong relationship to that security characteristic. If so, add an entry for that security characteristic mapping to that logical component's row in the table. By examining the mapping in both directions in this manner, security characteristic mappings are less likely to be overlooked or omitted.
6. Once these steps are complete, any rows in the table that don't have any mappings should be deleted.

The NCCoE applied this mapping process separately for each reference document. None of the mappings is intended to be exhaustive; they all focus on the strongest relationships involving each cybersecurity function in order to help organizations prioritize their work. Mapping every possible relationship, no matter how tenuous, would create so many mappings that they would not have any value in prioritization.

4 Mappings

The mappings are provided in the form of Excel files. Links to the mapping Excel files are organized in the remainder of this document as follows:

- Section 4.1 – NIST CSF 1.1 [2] and NIST CSF 2.0 [3] mappings. These include:
  - Section 4.1.1 – Mappings between reference design functions and NIST CSF Subcategories
  - Section 4.1.2 – Mappings between specific onboarding protocol (i.e., Wi-Fi Easy Connect and BRSKI) functions and NIST CSF Subcategories
  - Section 4.1.3 – Mappings between specific build functions and NIST CSF Subcategories
- Section 4.2 – NIST SP 800-53r5 [5] mappings. These include:
  - Section 4.2.1 – Mappings between reference design functions and NIST SP 800-53r5 controls

- Section 4.2.2 – Mappings between specific onboarding protocol (i.e., Wi-Fi Easy Connect and BRSKI) functions and NIST SP 800-53r5 controls
- Section 4.2.3 – Mappings between specific build functions and NIST SP 800-53r5 controls

4.1 NIST CSF Subcategory Mappings

This section provides links to mappings between various elements that provide trusted network-layer onboarding functionality and NIST CSF Subcategories.

4.1.1 Mappings Between Reference Design Functions and NIST CSF Subcategories

This Excel file provides mappings between the logical components of the reference design and the NIST CSF Subcategories. These mappings indicate how trusted IoT device network-layer onboarding and lifecycle management functions help support CSF Subcategories and vice versa.

Link to the Excel file called "IoT Volume E CSF 1-1 and 2-0", and to the tab called "CSF-to-Reference Arch" (first tab)

4.1.2 Mappings Between Specific Onboarding Protocols and NIST CSF Subcategories

This section provides mappings between the functionality provided by two network-layer onboarding protocols, Wi-Fi Easy Connect and BRSKI, and the NIST CSF Subcategories.

4.1.2.1 Mapping Between Wi-Fi Easy Connect and NIST CSF Subcategories

This Excel file provides a mapping between the functionality provided by the Wi-Fi Easy Connect protocol and the NIST CSF Subcategories. These mappings indicate how Wi-Fi Easy Connect functionality helps support CSF Subcategories and vice versa.

Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-Wi-Fi EasyCnct" (third tab)

4.1.2.2 Mapping Between BRSKI and NIST CSF Subcategories

This Excel file provides a mapping between the functionality provided by BRSKI and the NIST CSF Subcategories. These mappings indicate how BRSKI functionality helps support CSF Subcategories and vice versa.

Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-BRSKI" (second tab)

4.1.3 Mappings Between Specific Builds and NIST CSF Subcategories

This section provides mappings between the functionality provided by builds of the trusted IoT device network-layer onboarding and lifecycle management reference design that were implemented as part of this project and the NIST CSF Subcategories.

4.1.3.1 Mapping Between Build 1 and NIST CSF Subcategories

Build 1 is an implementation of network-layer onboarding that uses the Wi-Fi Easy Connect protocol. The onboarding infrastructure and related technology components for Build 1 have been provided by Aruba/HPE. IoT devices that were onboarded using Build 1 were provided by Aruba/HPE and CableLabs. The technologies used in Build 1 are detailed in Appendix C of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 1 components and CSF Subcategories. These mappings indicate how these components help support CSF Subcategories and vice versa.

Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-B1" (fourth tab)

4.1.3.2 Mapping Between Build 2 and NIST CSF Subcategories

Build 2 is an implementation of network-layer onboarding that uses the Wi-Fi Easy Connect protocol. The onboarding infrastructure and related technology components for Build 2 have been provided by CableLabs and OCF. IoT devices that were onboarded using Build 2 were provided by CableLabs, OCF, and Aruba/HPE. The technologies used in Build 2 are detailed in Appendix D of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 2 components and CSF Subcategories. These mappings indicate how these components help support CSF Subcategories and vice versa.

Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-B2" (fifth tab)

4.1.3.3 Mapping Between Build 3 and NIST CSF Subcategories

Build 3 is an implementation of network-layer onboarding that uses BRSKI. The onboarding infrastructure and related technology components for Build 3 have been provided by Sandelman Software Works. The IoT device that was used to demonstrate onboarding in Build 3 was a pledge simulator provided by Sandelman. The technologies used in Build 3 are detailed in Appendix E of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 3 components and CSF Subcategories. These mappings indicate how these components help support CSF Subcategories and vice versa.

Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-B3" (sixth tab)

4.1.3.4 Mapping Between Build 4 and NIST CSF Subcategories

Build 4 is an implementation of network-layer connection to an OpenThread network using pre-provisioned network credentials as well as independent application-layer onboarding using the Kudelski KeySTREAM service. The network infrastructure and related technology components for Build 4 have been provided by Silicon Labs and Kudelski. The IoT device that was used to demonstrate onboarding in Build 4 was provided by Silicon Labs. The technologies used in Build 4 are detailed in Appendix F of SP 1800-36B.

544 This Excel file details the mapping between the functionality provided by Build 4 components and CSF
545 Subcategories These mappings indicate how these components help support CSF Subcategories and vice
546 versa.

547 **Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-B4" (seventh tab)**

548 #### *4.1.3.5 Mapping Between Build 5 and NIST CSF Subcategories*

549 Build 5 is an implementation of network-layer onboarding using BRSKI over Wi-Fi, as well as
550 demonstration of a continuous authorization service. The network layer onboarding infrastructure and
551 related technology components for Build 5 have been provided by NquiringMinds. The IoT devices that
552 were used to demonstrate onboarding in Build 5 were provided by NquiringMinds. The technologies
553 used in Build 5 are detailed in Appendix G of SP 1800-36B.

554 This Excel file details the mapping between the functionality provided by Build 5 components and CSF
555 Subcategories. These mappings indicate how these components help support CSF Subcategories and
556 vice versa.

557 **Link to the Excel file called "CSF 1.1 and 2.0 Tables", and to the tab called "CSF-to-B5" (eighth tab)**

558 ## 4.2 NIST SP 800-53 Control Mappings

559 This section provides mappings between various elements that provide trusted network-layer
560 onboarding functionality and NIST SP 800-53 controls.

561 ### 4.2.1 Mappings Between Reference Design Functions and NIST SP 800-53 Controls

562 This Excel file provides a mapping between the logical components of the reference design and NIST SP
563 800-53 security controls. These mappings indicate how trusted IoT device network-layer onboarding and
564 lifecycle management functions help support NIST SP 800-53 controls. Because hundreds of NIST SP 800-
565 53 controls can help support these functions, we have limited use case 2 (see Section 3.1) mappings to
566 those controls on which specified supporting controls directly depend (e.g., dependence of
567 cryptographic protection on key management). Readers needing to determine how their trusted IoT
568 device network-layer onboarding and lifecycle management implementations support RMF processes
569 can refer to these mappings.

570 **Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-Reference Arch" (first tab)**

571 ### 4.2.2 Mappings Between Specific Onboarding Protocols and NIST SP 800-53
572 Controls

573 This section provides mappings between the functionality provided by specific network-layer
574 onboarding protocols and the NIST SP 800-53 controls. Mappings are provided for both the Wi-Fi Easy
575 Connect protocol and BRSKI.

4.2.2.1 Mapping Between Wi-Fi Easy Connect and NIST SP 800-53 Controls

This Excel file provides a mapping between the functionality provided by the Wi-Fi Easy Connect protocol and the NIST SP 800-53 controls. These mappings indicate how Wi-Fi Easy Connect functions help support NIST SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-Wi-Fi EasyCnct" (second tab)

4.2.2.2 Mapping Between BRSKI and NIST SP 800-53 Controls

This Excel file provides a mapping between the functionality provided by BRSKI and the NIST SP 800-53 controls. These mappings indicate how BRSKI functions help support NIST SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-BRSKI" (third tab)

4.2.3 Mappings Between Specific Builds and NIST SP 800-53 Controls

This section provides mappings between the functionality provided by builds of the trusted IoT device network-layer onboarding and lifecycle management reference design that were implemented as part of this project and the NIST SP 800-53 controls.

4.2.3.1 Mapping Between Build 1 and NIST SP 800-53 Controls

Build 1 is an implementation of network-layer onboarding that uses the Wi-Fi Easy Connect protocol. The onboarding infrastructure and related technology components for Build 1 have been provided by Aruba/HPE. IoT devices that were onboarded using Build 1 were provided by Aruba/HPE and CableLabs. The technologies used in Build 1 are detailed in Appendix C of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 1 components and SP 800-53 controls. These mappings indicate how these components help support SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-B1" (fourth tab)

4.2.3.2 Mapping Between Build 2 and NIST SP 800-53 Controls

Build 2 is an implementation of network-layer onboarding that uses the Wi-Fi Easy Connect protocol. The onboarding infrastructure and related technology components for Build 2 have been provided by CableLabs and OCF. IoT devices that were onboarded using Build 2 were provided by CableLabs, OCF, and Aruba/HPE. The technologies used in Build 1 are detailed in Appendix D of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 2 components and SP 800-53 controls These mappings indicate how these components help support SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-B2" (fifth tab)

4.2.3.3 Mapping Between Build 3 and NIST SP 800-53 Controls

Build 3 is an implementation of network-layer onboarding that uses BRSKI. The onboarding infrastructure and related technology components for Build 3 have been provided by Sandelman Software Works. The IoT device that was used to demonstrate onboarding in Build 3 was a pledge simulator provided by Sandelman. The technologies used in Build 3 are detailed in Appendix E of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 3 components and SP 800-53 controls. These mappings indicate how these components help support SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-B3" (sixth tab)

4.2.3.4 Mapping Between Build 4 and NIST SP 800-53 Controls

Build 4 is an implementation of network-layer connection to an OpenThread network using pre-provisioned network credentials as well as independent application-layer onboarding using the Kudelski KeySTREAM service. The network infrastructure and related technology components for Build 4 have been provided by Silicon Labs and Kudelski. The IoT device that was used to demonstrate onboarding in Build 4 was provided by Silicon Labs. The technologies used in Build 4 are detailed in Appendix F of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 4 components and SP 800-53 controls. These mappings indicate how these components help support SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-B4" (seventh tab)

4.2.3.5 Mapping Between Build 5 and NIST SP 800-53 Controls

Build 5 is an implementation of network-layer onboarding using BRSKI over Wi-Fi, as well as demonstration of a continuous authorization service. The network layer onboarding infrastructure and related technology components for Build 5 have been provided by NquiringMinds. The IoT devices that were used to demonstrate onboarding in Build 5 were provided by NquiringMinds. The technologies used in Build 5 are detailed in Appendix G of SP 1800-36B.

This Excel file details the mapping between the functionality provided by Build 5 components and SP 800-53 controls. These mappings indicate how these components help support SP 800-53 controls and vice versa.

Link to the Excel file called "800-53 Tables", and to the tab called "800-53-to-B5" (eighth tab)

Appendix A References

[1] K. Scarfone, M. Souppaya, and M. Fagan, Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Content Mappings, National Institute of Standards and Technology (NIST) Internal Report (IR) 8477, Gaithersburg, Md., August 2023, 26 pp. Available: https://doi.org/10.6028/NIST.IR.8477.ipd

[2] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

[3] National Institute of Standards and Technology, Version 2.0. The NIST Cybersecurity Framework 2.0 (CSF 2.0) (National Institute of Standards and Technology, Gaithersburg, MD), https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

[4] Executive Order 13800 (2017) Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (The White House, Washington, DC), DCPD-201700327, May 11, 2017. https://www.govinfo.gov/app/details/DCPD-201700327

[5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[6] S.2521 - Federal Information Security Modernization Act of 2014, 113th Congress (2013-2014), Became Public Law No: 113-283, December 18, 2014. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2521

[7] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2