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

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

William Barker
Dakota Consulting
Largo, Maryland

October 2023

SECOND PRELIMINARY 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, 112 pages, October 2023, 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: October 31, 2023 through December 15, 2023

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
Andy Dolan	CableLabs
Kyle Haefner	CableLabs
Craig Pratt	CableLabs
Darshak Thakore	CableLabs
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
Brecht Wyseur	Kudelski IoT
Faith Ryan	The MITRE Corporation
Nicholas Allot	NquiringMinds
Toby Ealden	NquiringMinds
Alois Klink	NquiringMinds
John Manslow	NquiringMinds
Antony McCaigue	NquiringMinds
Alexandru Mereacre	NquiringMinds
Craig Rafter	NquiringMinds

Name	Organization
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
Michael Richardson	Sandelman Software Works
Pedro Fuentes	SEALSQ, a subsidiary of WISeKey
Gweltas Radenac	SEALSQ, a subsidiary of WISeKey
Kalvin Yang	SEALSQ, a subsidiary of WISeKey
Mike Dow	Silicon Labs
Steve Egerter	Silicon Labs

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

List of Tables

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. Work continues on implementing

the example solutions and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

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. This is a preliminary draft guide. As the project progresses, the preliminary draft will be updated. 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

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 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] (Note: Future versions of this document are expected to map to *The NIST Cybersecurity Framework 2.0 (CSF 2.0).*) 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* [3], 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*) [4]. 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) [5]. Many other governments and private sector organizations voluntarily employ the Risk Management Framework [6] 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 organized in the remainder of this document as follows:

- Section 4.1 – NIST CSF 1.1 [2] 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 [4] 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 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

Table 4-1 provides mappings between the logical components of the reference design and the NIST CSF Subcategories. This table indicates how trusted IoT device network-layer onboarding and lifecycle management functions help support CSF Subcategories and vice versa.

Table 4-1 Mapping Between Reference Design Logical Components and NIST CSF Subcategories

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Creates, signs, and installs the device's unique identity and other birth credentials into secure storage. Installs info the device requires for application-layer onboarding (if applicable). Creates a record of devices that it has created.	Supports (example of) ID.AM-1: Physical devices and systems within the organization are inventoried	Information about the devices (e.g., device model, ID, onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		Is supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The device owner's expectations regarding the capabilities that the device should have (e.g., need for hardware-based secure storage, onboarding-specific firmware and software, and network- and application-layer onboarding credentials) must be clear before the manufacturer creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The manufacturer's factory provisioning process is responsible for generating and providing the device with a unique identity and credential (i.e., birth credential) that can be securely stored and cryptographically authenticated.
		Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	If the manufacturer installs device intent information (e.g., the device's Manufacturer Usage Description [MUD] URL) on the device, this information can be used by the network to configure access control lists (ACLs) on the router or switch to constrain communications to and from the device according to policy.
		Supports (integral to) PR.AC-6: Identities are	During factory provisioning, the device's unique identifier

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		proofed and bound to credentials and asserted in interactions	is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding.
Supply Chain Integration Service	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information to the device owner, and it may also be the mechanism for providing device ownership information to the device itself. Device bootstrapping information is information (e.g., a public key that pairs with the device's private key) that the device owner requires to perform trusted network-layer onboarding.	Supports (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Bootstrapping information for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
		Is supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The device owner's expectations regarding the mechanism for transferring the device bootstrapping information from the manufacturer to the device owner must be made clear so the manufacturer will use the expected mechanism (e.g., enrollment of the device's credential into a certificate authority [CA], direct transfer of the bootstrapping information into the device owner's database, or use of a QR

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			code that is imprinted on the device or its packaging).
		Supports (precedes) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
Network-Layer Onboarding Component	Runs the onboarding protocol to interact with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information. May interact with a certificate authority to sign the certificate provided to the device as part of the device's network credentials.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Bootstrapping information for all owned devices must be correlated with the device owner's inventory so that the bootstrapping information for the particular device being onboarded can be provided to the network-layer onboarding component. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
		Is supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The network-layer onboarding component of the device owner must be in possession of the device bootstrapping information in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the device owner must be defined,

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			well-understood, and trusted by both parties.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The network-layer onboarding service is responsible for providing authenticated, authorized devices with a network-layer credential.
		Supports (integral to) PR.AC-3: Remote access is managed	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The network-layer onboarding component is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
		Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	If device intent information is conveyed to the network onboarding component during the network-layer onboarding protocol exchange, the network onboarding component will forward this information to the appropriate network component so that ACLs can be configured on the router or switch to constrain communications to and from the device according to policy.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The network-layer onboarding component authenticates an IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The network-layer onboarding component authenticates the IoT device.
		Is supported by (example of) PR.AT-2: Privileged users understand their roles and responsibilities	In some network-layer onboarding protocols, participation of a trusted onboarder is required. This individual's role is to provide the device with the network's bootstrapping information and/or provide the network with the device's bootstrapping information. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The network-layer onboarding component establishes an encrypted channel with the IoT device

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Wireless access point (AP) and/or router or switch. The router may get configured with per-device ACLs and policy when devices are onboarded.	Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	When a device is onboarded, ACLs and policy for the device may be configured on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Network-Layer Onboarding Authorization Service	The authorization service provides the network onboarding component and router with the information needed to determine if the device is authorized to be onboarded to the network and, if so, whether it should be assigned any special roles or be subject to any specific access controls. The authorization service may also help enable the device to determine if the network is authorized to onboard it.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	An inventory of IoT devices belonging to the network owner must be available for the network-layer onboarding authorization service to consult in order for it to determine whether or not the device is authorized to be onboarded to the network.
IoT Device	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the onboarding protocol and interacts with the network onboarding	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The organization must have an inventory of the devices that support the particular trusted network-layer onboarding protocol to be used on the network (e.g., BRSKI or Wi-Fi Easy Connect)

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
	component to perform one-way or mutual authentication, establish a secure channel, and securely receive its network credentials. It may also have additional security capabilities, such as performing a secure boot process, performing trusted firmware updates, and securely conveying its device intent information.		so the organization knows which devices may be used.
		Is supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	If streamlined application-layer onboarding is supported, the device must either be provisioned with its application-layer bootstrapping information prior to network-layer onboarding or have the ability to generate one-time application-layer bootstrapping information at runtime. In either case, the organization must have an inventory of the devices with these capabilities so it knows which devices to use in cases in which it wants the device to perform application-layer onboarding.
		Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	When the device is equipped with device intent information (e.g., a MUD URL), the device conveys this information to the network where it can be used to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		and privacy risks and other organizational risks)	
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
Secure Storage	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to ensuring that the device's identity can be uniquely authenticated.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device's private key, which serves as its birth credential, is installed in secure storage within the device, thereby binding the device to its credential. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) PR.DS-1: Data-at-rest is protected	Information stored in secure storage is protected from unauthorized access and disclosure.
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (example of) PR.AC-1: Identities and credentials are issued,	The fact that a credential is signed by a trusted CA provides a mechanism that

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		managed, verified, revoked, and audited for authorized devices, users, and processes	may be used for enabling the credential to be verified and revoked.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	If the device credential is an X.509 certificate that is signed by a CA, this certificate binds the device's credential to the device's identity.
Application-Layer Onboarding Service	After the device connects to the network, this component interacts with the device using an application-layer onboarding protocol to authenticate the device, verify that it is authorized to be application-layer onboarded, establish a secure channel with it, and securely provision application-layer credentials to it. The application-layer credentials will allow the device to authenticate to an application-layer service. The application layer service may be a lifecycle management service that can be used to securely and automatically update and patch the device on an ongoing basis.	Is supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	In some application-layer onboarding mechanisms, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service.
		Supports (example of) ID.AM-2: Software platforms and applications within the organization are inventoried	The process of application-layer onboarding a device may serve as an automatic mechanism to inventory and keep track of which devices have application-related software installed and are therefore capable of interoperating with the application service.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The application-layer onboarding service is responsible for providing authenticated, authorized devices with an application-layer credential.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The application-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			of all information they exchange (e.g., the device's application-layer credentials).
Continuous Authorization Service	Performs a set of ongoing, policy-based assurance and authorization checks on the IoT device to support device lifecycle monitoring and control. For example, it may perform behavioral analysis or device attestation and use the results to determine whether the device should be granted access to certain high-value resources, assigned to a particular network segment, or other action taken.	Supports (example of) ID.RA-3: Threats, both internal and external, are identified and documented	The ongoing device authorization service may perform activities such as device attestation and behavioral analysis to identify potential threats.
		Supports (example of) ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	The ongoing device authorization service may perform policy-based authorization of devices based on behavioral analyses, device attestation, and other mechanisms.
		Supports (example of) ID.RA-6: Risk responses are identified and prioritized	The ongoing device authorization service may quarantine a device, refuse a device access to the network or to certain high-value resources, or take other pre-defined actions based on policy.
		Supports (example of) DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Behavioral analysis performed as part of ongoing device authorization may involve comparing observed activity against a baseline to detect anomalies and events.
		Supports (example of) DE.AE-3: Event data are collected and correlated from multiple sources and sensors	The ongoing device authorization service may collect and correlate data from device attestation services, behavioral analytics tools, authentication services, and other sources as input to its policy-based assessment of device authorization.

Logical Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		Supports (example of) DE.AE-5: Incident alert thresholds are established	If the policy-based assessment of the device does not meet certain policy criteria, the device may not be authorized to access specific resources or the network itself.
		Supports (example of) RS.MI-1: Incidents are contained	If the policy-based assessment of the device does not meet certain policy criteria, and, as a result, the device is denied access to the network or other resources, such restriction may help contain incidents that involve the device.

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

Table 4-2 provides a mapping between the functionality provided by the Wi-Fi Easy Connect protocol and the NIST CSF Subcategories. This table indicates how Wi-Fi Easy Connect functionality helps support CSF Subcategories and vice versa.

Table 4-2 Mapping Between Wi-Fi Easy Connect Functionality and NIST CSF Subcategories

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Installs the device's unique private/public key pair into secure storage, either by provisioning these credentials or having them autonomously generated. Creates the device's Device Provisioning Protocol (DPP)	Supports (example of) ID.AM-1: Physical devices and systems within the organization are inventoried	Information about the devices (e.g., device model, onboarding protocol supported, DPP URI) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
	URI (i.e., the device's bootstrapping information, which includes its public key) and makes a record of devices that it has created and their associated DPP URIs.		to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Is supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The requirements that the device must meet in order to support the Wi-Fi Easy Connect protocol and meet other trusted network- and application-layer onboarding expectations of its users must be clear to the manufacturer before it creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use. For example, the device will need hardware-based secure storage, Wi-Fi Easy Connect-specific firmware and software, support for one or more types of network credentials (e.g., connector, passphrase, X.509 certificate) and may need to be provisioned with or be equipped to generate bootstrapping information it will need to support streamlined application-layer onboarding.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited	The manufacturer's factory provisioning process is responsible for ensuring that the device is provisioned with or autonomously

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		for authorized devices, users, and processes	generates its own unique device credential in the form of a private/public key pair that is securely stored, as well as the DPP URI necessary for a configurator to cryptographically authenticate this device credential and then provide the device with its network-layer credential. Also, if the manufacturer provisions the device with application-layer onboarding bootstrapping information or equips the device with the capability to generate one-time application-layer bootstrapping information at runtime so that it can be provided to the configurator as a DPP configuration request object attribute within the Wi-Fi Easy Connect protocol, this enables the device to be securely provisioned with application-layer credentials as well.
		Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	If the manufacturer installs the device's MUD URL on the device so that it can be provided to the configurator as a DPP configuration request object attribute within the Wi-Fi Easy Connect protocol, this enables the network to use the device intent information that is in the MUD file to configure ACLs on the router or switch to constrain communications to and from

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			the device according to policy.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device credential that is provisioned or autonomously generated during the device manufacture and provisioning process (i.e., the device's unique private/public key pair) is stored in hardware-based secure storage. Possession of this unique private key is what enables the device to have its asserted identity authenticated during onboarding.
Supply Chain Integration Service	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information (e.g., the DPP URI) to the device owner. When using Wi-Fi Easy Connect, the device's public key, which is encoded in the DPP URI, is the device bootstrapping information that the device owner requires in order to authenticate the device, establish a secure connection to it, and proceed with the remainder of the trusted network-layer onboarding process.	Supports (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Bootstrapping information (e.g., the DPP URI) for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory so the owner will be able to authenticate the devices.
		Is supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The device owner's expectations regarding the mechanism for transferring the device bootstrapping information (i.e., the DPP URI) from the manufacturer to the device owner must be made clear so the manufacturer will use the expected mechanism (e.g., direct transfer of the bootstrapping information into the device owner's database, use of a QR code encoding of the DPP URI that is imprinted on the device or its packaging, encrypted

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			email listing device and DPP URI).
		Supports (precedes) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The generation and transfer of device bootstrapping information (i.e., the DPP URI) from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
Configurator (Network-Layer Onboarding Component)	Runs the onboarding protocol to interact with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information. May interact with a certificate authority to sign the certificate provided to the device as part of the device's network credentials.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The DPP URI for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory so the owner will be able to authenticate the devices.
		Is supported by (precedes) ID.BE-1: The organization's role in the supply chain is identified and communicated	The configurator of the device owner must be in possession of the device bootstrapping information (i.e., the DPP URI) in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the configurator via the device owner must be defined, well-understood, and trusted by both parties.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The configurator is responsible for provisioning authenticated, authorized devices with their network-layer credentials. In addition, when the device uses the DPP configuration request

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			object to securely convey its application-layer onboarding bootstrapping information in support of streamlined application-layer onboarding (e.g., via the OCF Information configuration attribute or other optional third-party attributes), the configurator also supports the secure provisioning of application-layer credentials.
		Supports (integral to) PR.AC-3: Remote access is managed	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The configurator is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
		Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	When the device uses the optional DPP configuration request object MUD URL attribute to securely convey its MUD URL to the configurator, the configurator supports use of the device intent information that is in the MUD file to configure ACLs on the router or switch that constrain communications to and from the device according to policy.

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The configurator authenticates an IoT device's identity by using the device's public key to verify that the corresponding unique private key is installed on the device.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The configurator authenticates the IoT device.
		Is supported by (example of) PR.AT-2: Privileged users understand their roles and responsibilities	When using Wi-Fi Easy Connect, participation of a trusted onboarder may be required. This individual's role is to provide the device with the network's bootstrapping information and/or provide the network with the device's bootstrapping information. For example, this person may scan the QR codes for the devices to be onboarded and upload them to a database. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device. This trusted onboarder is not privy to any private keys held

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			by the device or the network, but this onboarder must be trusted to ensure that the device is being onboarded to the appropriate, authorized network.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The configurator establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials, device intent information, application-layer bootstrapping information).
Access Point, Router, or Switch	Wireless access point and/or router or switch. The Wi-Fi Easy Connect protocol supports secure conveyance of device intent information (e.g., the device's MUD URL) to the configurator. This MUD URL may be used by the network to configure per-device ACLs and policy when devices are onboarded.	Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Wi-Fi Easy Connect uses special pre-association action frames. Until the device is authenticated and onboarded, the only 802.11 frames that are allowed from the device are these action frames; no other traffic is permitted. After the device is onboarded, all traffic is permitted, with the following caveat: if device intent or other policy information for the device was securely conveyed by the Wi-Fi Easy Connect protocol, this information may be used to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) PR.AC-5: Network integrity is protected (e.g., network	Wi-Fi Easy Connect uses special pre-association action frames. Until the device is authenticated and onboarded, the only 802.11

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		segregation, network segmentation)	frames that are allowed from the device are these action frames; no other traffic is permitted. When a device is onboarded, device intent or other policy information for the device that is securely conveyed by the Wi-Fi Easy Connect protocol may be used to configured ACLs on the router in a way that essentially assigns the device to a particular network segment.
Enrollee (IoT Device)	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the Wi-Fi Easy Connect protocol and interacts with the configurator to perform one-way or mutual authentication, establish a secure channel, and securely receive its network credentials. It may also have additional security capabilities, such as securely conveying its device intent information or its application-layer onboarding bootstrapping information (e.g., via the DPP configuration request object)	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The organization must have an inventory of the devices that support Wi-Fi Easy Connect onboarding so it knows which devices to use in cases in which it wants to use this protocol to perform trusted network-layer onboarding.
		Is supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	If streamlined application-layer onboarding is supported, the device must either be provisioned with its application-layer bootstrapping information prior to network-layer onboarding or have the ability to generate one-time application-layer bootstrapping information at runtime. In either case, the organization must have an inventory of the devices with these capabilities so it knows which ones to use in cases in which it wants the device to perform application-layer onboarding.

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	When the device is equipped with a MUD URL and uses the optional DPP configuration request object MUD URL attribute to securely convey this MUD URL to the configurator, the device intent information that is in the MUD file can be used to configure ACLs on the router or switch that constrain communications to and from the device according to policy.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The IoT device establishes an encrypted channel with the configurator to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g.,

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			the device's application-layer credentials).
Secure Storage	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The confidentiality provided to a device's private key by storing and using it in secure storage is essential to ensuring that the device's identity can be uniquely authenticated. Storing the device's network credentials in secure storage ensures their confidentiality.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device's private key, which serves as its birth credential, is installed in secure storage within the device, thereby binding the device to its credential. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) PR.DS-1: Data-at-rest is protected	Information stored in secure storage is protected from unauthorized access and disclosure.
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (example of) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Network-layer credentials provisioned by Wi-Fi Easy Connect may be signed by a trusted CA, enabling them to be verified and revoked. Note that although it is not an X.509 certificate and not related to a CA, a Wi-Fi Easy Connect connector is a signed public key. The signee is the configurator, which is trusted by all devices that are onboarded to the network. When the DPP configurator issues a connector, it signs the enrollee's protocol key to construct the connector. So,

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			the connector is a public key signed by a trusted 3rd party (the configurator), but it is not specific to a CA.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	If the network-layer credential that is provisioned is an X.509 certificate, then it will be signed by a CA, and asserted by the device in order to gain access to the network.

4.1.2.2 Mapping Between BRSKI and NIST CSF Subcategories

Table 4-3 provides a mapping between the functionality provided by BRSKI and the NIST CSF Subcategories. This table indicates how BRSKI functionality helps support CSF Subcategories and vice versa.

Table 4-3 Mapping Between BRSKI Functionality and NIST CSF Subcategories

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Installs/generates the device's unique private key into secure storage and creates the associated signed 802.1AR certificate (i.e., the device's IDevID). Provides the location of the device's manufacturer authorized signing authority (MASA) in an extension to the IDevID. Provides the device with trust anchors for the MASA entity that will sign the returned vouchers. Installs info the device requires for application-layer onboarding (if applicable). Create a record of devices that it has created.	Supports (example of) ID.AM-1: Physical devices and systems within the organization are inventoried	Information about the devices (e.g., device model, ID, onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Is supported by (precedes) ID.BE-1:	The requirements that the device must meet in order

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
		The organization's role in the supply chain is identified and communicated	to support the BRSKI protocol and meet other trusted network- and application-layer onboarding expectations of its users must be clear to the manufacturer before it creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use. For example, the device will need hardware-based secure storage, BRSKI-specific firmware and software, and an 802.1AR certificate (e.g., connector, passphrase, X.509 certificate) and may need to be provisioned with or be equipped to generate bootstrapping information it will need to support streamlined application-layer onboarding.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The manufacturer's factory provisioning process is responsible for ensuring that the device is provisioned with or autonomously generates its own unique device credential in the form of an 802.1AR certificate (IDevID) and a private/public key pair that are securely stored so that the identity of the device can be cryptographically authenticated and then provided with its network-

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
			layer credential. Also, if the manufacturer provisions the device with application-layer onboarding bootstrapping information or equips the device with the capability to generate one-time application-layer bootstrapping information at runtime, this enables the device to be securely provisioned with application-layer credentials as well.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	During factory provisioning, the device's 802.1AR certificate (IDevID) is bound to its private key, which is stored in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding.
MASA (Supply Chain Integration Service)	The device manufacturer stores the device's serial number and IDevID in the MASA's database. When the device is sold, the manufacturer may also record the device owner information in the MASA. Storing this information in the MASA serves a mechanism whereby the device manufacturer transfers device bootstrapping information (i.e., the device's public key) to the device owner, as well as the mechanism for providing device ownership	Supports (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Bootstrapping information (e.g., an 802.1AR certificate) for each of the devices that the manufacturer creates must be provided to the domain registrar of the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded in the MASA in order for the device to determine whether the

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
	information to the device itself. The MASA consults its stored information and applies policy to determine whether or not to approve a registrar's claim that it owns a device. If so, it creates and signs a voucher that directs the device to accept its new owner and sends it back to the registrar.		network is authorized to onboard the device.
		Supports (precedes) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The generation and transfer of device bootstrapping information (e.g., device certificate information) from the device manufacturer to the device owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. Also, the transfer of device ownership information from the device owner to the device must occur before the device will permit itself to be onboarded to the network. The transfer of this ownership and bootstrapping information is achieved by storing the device ownership information in a trusted MASA and having the MASA generate a signed voucher attesting to device ownership assertions.
Domain Registrar (Network-Layer Onboarding Component and Network-Layer Onboarding Authorization Service)	Runs the BRSKI onboarding protocol to interact with the IoT device and the MASA. This involves performing one-way or mutual authentication, establishing a secure channel, and securely providing local network credentials to the device. Also provides an authorization function. Prior to permitting the	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The certificate for each of the devices that the manufacturer creates, along with information regarding which organization owns each device is provided to the MASA. The domain registrar relies on the MASA to approve the registrar's claim that it owns a device. This claim approval will be based on

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
	device to be onboarded, it examines the pledge voucher request provided by the IoT device and determines whether the device's manufacturer is known to it and whether devices of that type are welcome on the network. As part of its authorization service, it also helps the device to determine whether the network is authorized to onboard it (by serving as an intermediary for the vouchers exchanged between the device and the MASA).		the fact that the MASA has been provided with a list of devices that are owned by the network. This list of device certificates constitutes an inventory of the organization's devices that must be in the MASA prior to onboarding.
		Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The domain registrar is responsible for providing authenticated, authorized devices with a network-layer credential.
		Supports (integral to) PR.AC-3: Remote access is managed	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The domain registrar is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The domain registrar authenticates an IoT device's identity by using the device's public key to verify that the device's

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
			private key is installed on the device.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The domain registrar authenticates the IoT device.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The domain registrar establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Wireless access point and/or router or switch. The router may get configured with per-device ACLs and policy when devices are onboarded.	Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	When a device is onboarded, ACLs and policy for the device may be configured on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Pledge (IoT Device)	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs	Is supported by (precedes) ID.AM-1: Physical devices and systems within the	The organization must have an inventory of the devices that support BRSKI onboarding so it knows

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
	the onboarding protocol and interacts with the network onboarding component to perform one-way or mutual authentication, establish a secure channel, and securely request and receive its network credentials. It also interacts with the MASA via signed vouchers sent to and received from the domain registrar to ensure that the network that is trying to onboard it is authorized to do so before permitting itself to be onboarded.	organization are inventoried	which devices to use in cases in which it wants to use this protocol to perform trusted network-layer onboarding.
		Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		Supports (integral to) PR.DS-2: Data-in-transit is protected	The IoT device establishes an encrypted channel with the domain registrar to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
Secure Storage	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to ensuring that

BRSKI Component	Component's Function	Function's Relationships to BRSKI Subcategories	Relationship Explanation
	contents. Used to store and process the device's private key (IDevID), network credentials (LDevID), and any other information that must be kept confidential.	authorized devices, users, and processes	the device's identity can be uniquely authenticated.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device's private key, which serves as its birth credential along with its 802.1AR certificate (IDevID), is installed in secure storage within the device, thereby binding the device to its credential.
		Supports (integral to) PR.DS-1: Data-at-rest is protected	Information stored in secure storage is protected from unauthorized access and disclosure.
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (example of) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Network-layer credentials provisioned by BRSKI are signed by a trusted CA, enabling them to be verified and revoked.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device credential is an 802.1AR certificate (e.g., an IDevID) that is signed by a CA. This certificate binds the device's credential to the device's identity. Also, all vouchers exchanged as part of the protocol are signed, enabling claims regarding device ownership to be verified. Also, the pledge and domain registrar create and sign voucher requests using their certificates, which in turn were signed by the CA.

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. Mappings are provided only for Build 1 at this time.

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.

Table 4-4 details the mapping between the functionality provided by Build 1 components and CSF Subcategories. It indicates how these components help support CSF Subcategories and vice versa.

Table 4-4 Mapping Between Functionality of Build 1 Components and NIST CSF Subcategories

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
Supply Chain Integration Service	Aruba Central	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information to the device owner. The manufacturer provides device bootstrapping information to the HPE Cloud via the Representational State Transfer (REST) application programming interface (API) that is documented in the DPP specification. Once the device is transferred to an owner, the HPE Cloud provides the device bootstrapping information (i.e., the	Supports (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Bootstrapping information for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
			Is supported by (precedes) ID.BE-1: The organization's role in the supply	The device owner's expectations regarding the mechanism for transferring the device bootstrapping

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		device's DPP URI) to the device owner's private tenancy within the HPE Cloud. Device bootstrapping information is information (e.g., a public key that pairs with the device's private key) that the device owner requires to perform trusted network-layer onboarding.	chain is identified and communicated	information from the manufacturer to the device owner must be made clear so the manufacturer will use the expected mechanism (e.g., enrollment of the device's credential into a CA, direct transfer of the bootstrapping information into the device owner's database, or use of a QR code that is imprinted on the device or its packaging).
			Supports (precedes) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
Network-Layer Onboarding Component	Aruba Access Point with support from Aruba Central	Runs the Wi-Fi Easy Connect network-layer onboarding protocol to interact with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The DPP URI for each of the devices must be provided to the device owner and correlated with the devices in the owner's inventory so the owner will be able to authenticate the devices.
			Is supported by (precedes) ID.BE-1: The organization's	The configurator of the device owner must be in possession of the

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		device. If the network credential that is being provided to the device is a certificate, the onboarding component will interact with a certificate authority to sign the certificate. The configurator deployed in Build 1 supports DPP 2.0, but it is also backward compatible with DPP 1.0.	role in the supply chain is identified and communicated	device bootstrapping information (i.e., the DPP URI) in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the configurator via the device owner must be defined, well-understood, and trusted by both parties.
			Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The network-layer onboarding service is responsible for providing authenticated, authorized devices with a network-layer credential.
			Supports (integral to) PR.AC-3: Remote access is managed	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The configurator is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
				fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
			Supports (integral to) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	The only traffic the AP will permit being sent prior to onboarding is DPP action frames. All other traffic is dropped.
			Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The configurator authenticates an IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
			Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The configurator authenticates the IoT device.
			Is supported by (example of) PR.AT-2: Privileged users understand	In this build, participation of a trusted onboarder is optional. When

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			their roles and responsibilities	present, this individual's role is to provide the network with the device's bootstrapping information by uploading the device's DPP URIs to a database. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device.
			Supports (integral to) PR.DS-2: Data-in-transit is protected	The configurator establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Aruba Access Point	Wireless access point that also serves as a router. It may get configured with per-device ACLs and policy when devices are onboarded.	Supports (example of) PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	The only traffic the AP will permit being sent prior to onboarding is DPP action frames. All other traffic is dropped. When a device is onboarded, ACLs and policy for the device may be configured on the router to constrain communications to and from the device according to policy.
			Supports (example of) PR.AC-5: Network integrity is protected (e.g.,	Wi-Fi Easy Connect uses special pre-association action frames. Until the device

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			network segregation, network segmentation)	is authenticated and onboarded, the only 802.11 frames that are allowed from the device are these action frames; no other traffic is permitted. When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Network-Layer Onboarding Authorization Service	Cloud Auth (on Aruba Central)	The authorization service provides the configurator and router with the information needed to determine if the device is authorized to be onboarded to the network and, if so, whether it should be assigned any special roles or be subject to any specific access controls. It provides device authorization, role-based access control, and policy enforcement.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	An inventory of IoT devices belonging to the network owner must be available for the network-layer onboarding authorization service to consult in order for it to determine whether or not the device is authorized to be onboarded to the network.
Build-specific IoT Device	Aruba UXI Sensor	The IoT device that is used to demonstrate both trusted network-layer onboarding and trusted application-layer onboarding. It runs the Wi-Fi Easy Connect network-layer onboarding protocol supported	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The organization must have an inventory of the devices that support Wi-Fi Easy Connect network-layer onboarding so it knows which devices to use in cases in which it wants to use this protocol.
			Is supported by (precedes) ID.AM-	To support UXI application-layer

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
		by the build to securely receive its network credentials. It also has an application that enables it to perform independent application-layer onboarding.	2: Software platforms and applications within the organization are inventoried	onboarding, the device must have been provisioned with its application-layer bootstrapping information and software prior to network-layer onboarding. The organization must have an inventory of the devices with this UXI application-layer onboarding capability so it knows which devices to use in cases in which it wants the device to perform application-layer onboarding.
			Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The IoT device permits itself to be authenticated as part of the network-layer onboarding process.
			Supports (integral to) PR.DS-2: Data-in-transit is protected	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
				exchange (e.g., the device's network-layer credentials). In support of UXI application-layer onboarding, the IoT device establishes an encrypted channel with the application-layer onboarding service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
Generic IoT Device	Raspberry Pi	The IoT device that is used to demonstrate only trusted network-layer onboarding.	Is supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	The organization must have an inventory of the devices that support Wi-Fi Easy Connect network-layer onboarding so it knows which devices to use in cases in which it wants to use this protocol.
			Supports (integral to) PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	The IoT device permits itself to be authenticated as part of the network-layer onboarding process.
			Supports (integral to) PR.DS-2: Data-in-transit is protected	The IoT device establishes an encrypted channel with the network-layer

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
				onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). To support application-layer onboarding, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of in-formation exchanged (e.g., the device's application-layer credentials).
Secure Storage	Aruba UXI Sensor Trusted Platform Module (TPM)	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.	Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to ensuring that the device's identity can be uniquely authenticated.
			Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	The device's private key, which serves as its birth credential, is installed in secure storage within the device, thereby binding the device to its credential.
			Supports (integral to) PR.DS-1: Data-at-rest is protected	Information stored in secure storage is protected from unauthorized access and disclosure.
	Private CA		Supports (example of) PR.AC-1:	Network-layer credentials provisioned

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
Certificate Authority (CA)		Issues and signs certificates as needed.	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	by this build may be signed by a trusted CA, enabling them to be verified and revoked.
			Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	If the network-layer credential that is provisioned is an X.509 certificate, then it will be signed by a CA and asserted by the device in order to gain access to the network.
Application-Layer Onboarding Service	UXI Application and UXI Cloud	After connecting to the network, the device downloads its application-layer credentials from the UXI cloud and uses these to authenticate to the UXI application with which it interacts.	Is supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	To support UXI application-layer onboarding, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service.
			Supports (integral to) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The application-layer onboarding service is responsible for providing authenticated, authorized devices with an application-layer credential.
			Supports (integral to) PR.DS-2: Data-	The application-layer onboarding component

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to CSF Subcategories	Relationship Explanation
			in-transit is protected	establishes an encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).

4.2 NIST SP 800-53 Control Mappings

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

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

Table 4-5 provides a mapping between the logical components of the reference design and NIST SP 800-53 security controls. This table indicates how trusted IoT device network-layer onboarding and lifecycle management functions help support NIST SP 800-53 controls. Because hundreds of NIST SP 800-53 controls can help support these functions, we have limited use case 2 (see Section 3.1) mappings to those controls on which specified supporting controls directly depend (e.g., dependence of cryptographic protection on key management). Readers needing to determine how their trusted IoT device network-layer onboarding and lifecycle management implementations support RMF processes can refer to the SP 800-53 mappings in Table 4-5.

Table 4-5 Mapping Between Reference Design Logical Components and NIST SP 800-53 Controls

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Creates, signs, and installs the device's unique identity and other birth credentials into secure storage. Installs info the device requires for application-layer onboarding (if applicable). Creates a record of devices that it has created.	Supports (example of) AC-3: Access Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. When the device is sold, the information will be provided to the device owner. The owner may use this information as the basis of the owner's implementation of connections to the device. If the manufacturer installs device intent information (e.g., the device's MUD URL) on the device, this information can be used by the network to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) AC-4: Information Flow Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided to the device owner. The owner may use this information as the basis of the owner's implementation of connections enabling information transmitted by the device. If the manufacturer installs device intent information (e.g., the device's MUD URL) on the device, this information can be used by the network to configure ACLs on the router or switch to

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			constrain communications to and from the device according to policy.
		Supports (example of) AC-6: Least Privilege	If the manufacturer installs device intent information (e.g., the device's MUD URL) on the device, this information can be used by the network to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) CM-8: System Component Inventory	Information about the devices (e.g., device model, ID, onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Supports (integral to) IA-3: Device Identification and Authentication	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding.
		Supports (precedes) IA-9: Service	In some application-layer onboarding mechanisms, the IoT device must be prepared

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Identification and Authentication	for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service. Signed information about the device (e.g., device model, ID, onboarding protocol supported) created and provided by the manufacturer during the factory provisioning process is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices.
		Supports (precedes) PM-5: System Inventory	The owner uses this information in compiling the owner's organization-wide inventories information that includes devices obtained from that manufacturer.
		Supports (precedes) SR-4: Provenance	Creation, signing, and installation of the device's unique identity and other birth credentials into secure storage and creation of records of devices that the manufacturer has created support documentation and maintenance of the valid provenance of system components. During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			is what enables the device to have its asserted identity authenticated during onboarding.
		Supports (example of) SR-5: Acquisition Strategies, Tools, and Methods	The signed device identities and records of manufactured devices can be required in acquisition and procurement documents to protect against and mitigate supply chain risks.
		Supports (example of) SR-11: Component Authenticity	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. Signing and installing the device's unique identity and other birth credentials into secure storage supports implementation of anti-counterfeiting policies and procedures by providing means to detect counterfeit components and prevent them from entering the system.
		Is supported by (example of) IA-1: Identification and Authentication Policy and Procedures	Customer policies regarding device access and information flows inform the manufacturer's decisions regarding information to be provided about the device's requirements for application-layer onboarding (e.g., onboarding protocol supported) and recording by the manufacturer during the factory provisioning process. When the device is sold, this

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			information may be provided to the device owner. The owner may use this information as the basis for acquisition, installation, and onboarding decisions.
		Is supported by (precedes) IA-4: Identifier Management	Management of device identifiers communicates to the manufacturer component identification information used to enable a record of devices that it has created to be used to support conformance to acquisition policies and notification agreements.
		Is supported by (precedes) SR-8: Notification Agreements	The role of the manufacturer as established in notification agreements with entities involved in the supply chain for systems components must be made clear before it performs factory provisioning so the manufacturer can understand what onboarding-specific hardware, firmware, and software it must integrate into the device.
Supply Chain Integration Service	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information to the device owner, and it may also be the mechanism for providing device ownership information to the device itself. Device bootstrapping information is information (e.g., a public key that pairs with the device's private key) that the device owner	Supports (precedes) AC-3: Access Enforcement	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Supports (precedes) AC-4: Information Flow Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
	requires to perform trusted network-layer onboarding.		recorded by the manufacturer during the factory provisioning process. Note that the generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Supports (integral to) CM-8: System Component Inventory	Bootstrapping information for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
		Supports (example of) IA-1: Identification and Authentication Policy and Procedures	Cryptographically authenticating devices during network-layer onboarding to the device owner's network can facilitate an organization's identification and authentication policies and procedures regarding network connections to IoT devices. The network-layer credentials that are provisioned are unique to the device and can be used to

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			identify devices on the network after onboarding has finished.
		Supports (integral to) IA-3: Device Identification and Authentication	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Supports (precedes) IA-9: Service Identification and Authentication	Signed device bootstrapping information is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices.
		Supports (precedes) PM-5: System Inventory	The device owner uses the bootstrapping information in compiling the owner's organization-wide inventory information that includes devices obtained from that manufacturer.
		Supports (precedes) SR-4: Provenance	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. Creation, signing, and installation of the device's unique identity and other birth credentials into secure storage and creation of records of devices that the manufacturer has created

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			support documentation and maintenance of the valid provenance of system components.
		Supports (example of) SR-5: Acquisition Strategies, Tools, and Methods	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. These signed device identities and records of manufactured devices can be required in acquisition and procurement documents to protect against and mitigate supply chain risks.
		Supports (example of) SR-11: Component Authenticity	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. Signing and installing the device's unique identity and other birth credentials into secure storage may support implementation of anti-counterfeiting policies and procedures by providing means to detect counterfeit components and prevent them from entering the system.
		Is supported by (precedes) SR-1: Supply Chain Risk	The device owner's expectations regarding the mechanism for transferring the

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Management Policy and Procedures	device bootstrapping information from the manufacturer to the device owner are informed by supply chain risk management policies and procedures so that the manufacturer can use expected mechanisms to enable policy enforcement (e.g., enrollment of the device's credential into a CA, direct transfer of the bootstrapping information into the device owner's database, or use of a QR code that is imprinted on the device or its packaging).
Network-Layer Onboarding Component	Runs the onboarding protocol to interact with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information. May interact with a certificate authority to sign the certificate provided to the device as part of the device's network credentials.	Supports (integral to) AC-1: Access Control Policy and Procedures	The network-layer onboarding service supports implementation of access control policies and procedures by providing authenticated, authorized devices with a network-layer credential.
		Supports (integral to) AC-3: Access Enforcement	The network-layer onboarding component supports access enforcement by authenticating a connected IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
		Supports (example of) AC-6: Least Privilege	If device intent information is conveyed to the network onboarding component during the network-layer onboarding protocol exchange, the network onboarding component will forward this information to the appropriate network component so that ACLs can be configured on the router or switch to constrain

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			communications to and from the device according to policy.
		Supports (integral to) AC-17: Remote Access	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The network-layer onboarding component is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices. Also, the provisioned credentials are unique.
		Supports (example of) AC-19: Access Control for Mobile Devices	Where the IoT device is a mobile device, remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely.
		Supports (integral to) AC-20: Use of External Systems	Access to the network from external systems is managed by ensuring that only devices that have network-layer credentials are permitted to connect to external systems.
		Supports (integral to) AC-24: Access Control Decisions	Access control decisions are enforced by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely.
		Is supported by (precedes CM-8: System	Bootstrapping information for all owned devices must be correlated with the device

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Component Inventory	owner's inventory so that the bootstrapping information for the particular device being onboarded can be provided to the network-layer onboarding component. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard it.
		Supports (integral to) IA-1: Identification and Authentication Policy and Procedures	The network-layer onboarding service provides a network-layer credential for authentication of authorized devices.
		Supports (integral to) IA-3: Device Identification and Authentication	The network-layer onboarding service provides a network-layer credential for authentication of authorized devices. Before provisioning a device with its network-layer credentials, the configurator authenticates the device using the device's bootstrapping information.
		Supports (precedes) IA-9: Service Identification and Authentication	Signed information about the device (e.g., device model, ID, onboarding protocol supported) created and provided by the manufacturer during the factory provisioning process is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices. The network-layer onboarding service supports

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			service identification and authentication by providing a network-layer credential for authentication of authorized devices.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The network-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
		Supports (integral to) SC-15: Collaborative Computing Devices and Applications	When a device is onboarded, ACLs and policy for the device are configured on the router or switch to constrain communications to and from the device according to policy.
		Is supported by (precedes) SR-1: Supply Chain Risk Management Policy and Procedures	The network-layer onboarding component of the device owner must be in possession of the device bootstrapping information in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the device owner must be consistent with both manufacturer and customer supply chain risk management policies and procedures.
		Is supported by (example of) AT-3: Role-Based Training	In some network-layer onboarding protocols, participation of a trusted onboarder is required. This individual's role is to provide the device with the network's bootstrapping information and/or provide the network

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			with the device's bootstrapping information. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device.
		Is supported by (integral to) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the network-layer onboarding component's establishment of an encrypted channel with the IoT device in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Wireless access point and/or router or switch. The router may get configured with per-device ACLs and policy when devices are onboarded.	Supports (example of) AC-4: Information Flow Enforcement	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment, thus enforcing approved authorizations for controlling the flow of information within the system and between connected systems based on organization-defined information flow control policies.
		Supports (example of) AC-5: Separation of Duties	When a device is onboarded, ACLs and policy for the device may be configured on the router or switch to constrain communications to and from the device according to separation of duties policies.
		Supports (example of) AC-6: Least Privilege	When a device is onboarded, ACLs and policy for the device may be configured on the

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			router or switch to constrain communications to and from the device according to least privilege policies.
		Supports (example of) AC-16: Security and Privacy Attributes	When a device is onboarded, ACLs and policy for the device may be configured on the router or switch to constrain communications to and from the device consistent with policies regarding permitted security and privacy attributes.
		Supports (integral to) AC-17: Remote Access	When a device is onboarded, ACLs and policy for the device are configured on the router or switch to constrain communications to and from the device.
		Supports (integral to) AC-24: Access Control Decisions	When a device is onboarded, ACLs and policy for the device are configured on the router or switch to control decisions regarding communications to and from the device.
		Supports (example of) SC-7: Boundary Protection	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Network-Layer Onboarding Authorization Service	The authorization service provides the network onboarding component and router with the information needed to determine if the device is authorized to be onboarded to the network and, if so, whether it should be assigned any special roles or be subject to any specific access controls. The authorization service may also help enable the device	Is supported by (precedes) CM-8: System Component Inventory	An inventory of IoT devices belonging to the network owner must be available for the network-layer onboarding authorization service to consult in order for it to determine whether or not the device is authorized to be onboarded to the network.

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
	to determine if the network is authorized to onboard it.		
IoT Device	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the onboarding protocol and interacts with the network onboarding component to perform one-way or mutual authentication, establish a secure channel, and securely receive its network credentials. It may also have additional security capabilities, such as performing a secure boot process, performing trusted firmware updates, and securely conveying its device intent information.	Supports (example of) AC-6: Least Privilege	When the device is equipped with device intent information (e.g., a MUD URL), the device conveys this information to the network where it can be used to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (integral to) IA-3: Device Identification and Authentication	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		Is supported by (precedes) CM-8: System Component Inventory	The organization must have an inventory of the devices that support the particular trusted network-layer onboarding protocol to be used on the network (e.g., BRSKI or Wi-Fi Easy Connect) so the organization knows which devices may be used. If streamlined application-layer onboarding is supported, the device must either be provisioned with its application-layer bootstrapping information prior to network-layer onboarding or have the ability to generate one-time application-layer bootstrapping information at runtime. In either case, the organization must have an inventory of the devices with these capabilities so it knows which devices to

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			use in cases in which it wants the device to perform application-layer onboarding.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
		Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Secure Storage	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.	Supports (integral to) AC-1: Access Control Policy and Procedures	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to implementation of the organization's access control policy.
		Supports (integral to) IA-1: Policy and Procedures	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to the effective

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			implementation of the organization's identification and authentication policies as they relate to IoT.
		Supports (integral to) AC-3: Access Enforcement	The secure storage of the device's private key, which serves as its birth credential within the device and binds the device to its credential, is an essential element of the access enforcement mechanism.
		Supports (integral to) IA-3: Device Identification and Authentication	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to the effectiveness and security of device identification and authentication processes. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) SC-28: Protection of Information at Rest	Information stored in secure storage is protected from unauthorized access and disclosure.
		Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (integral to) IA-3: Device Identification and Authentication	If the device credential is an X.509 certificate that is signed by a trusted CA, this certificate binds the device's credential to

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			the device's identity. It provides a mechanism for enabling the credential to be verified and revoked that is essential to the integrity of the authentication process.
		Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Application-Layer Onboarding Service	After the device connects to the network, this component interacts with the device using an application-layer onboarding protocol to authenticate the device, verify that it is authorized to be application-layer onboarded, establish a secure channel with it, and securely provision application-layer credentials to it. The application-layer credentials will allow the device to authenticate to an application-layer service. The application layer service may be a lifecycle management service that can be used to securely and automatically update and patch the device on an ongoing basis.	Supports (example of) AC-18: Wireless Access	The application-layer onboarding component may establish a wireless encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
		Supports (integral to) IA-3: Device Identification and Authentication	The application-layer onboarding service is responsible for providing authenticated, authorized devices with an application-layer credential.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The application-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
		Is supported by (precedes) CM-8: System	In some application-layer onboarding mechanisms, the IoT device must be prepared

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Component Inventory	for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service. The process of application-layer onboarding a device may also serve as an automatic mechanism to inventory and keep track of which devices have application-related software installed and are therefore capable of interoperating with the application service.
Continuous Authorization Service	Performs a set of ongoing, policy-based assurance and authorization checks on the IoT device to support device lifecycle monitoring and control. For example, it may perform behavioral analysis or device attestation and use the results to determine whether the device should be granted access to certain high-value resources, assigned to a particular network segment, or other action taken.	Supports (example of) RA-2: Security Categorization	The ongoing device authorization service may perform activities such as device attestation and behavioral analysis to identify the impact of system security breaches.
		Supports (example of) RA-3: Risk Assessment	The ongoing device authorization service may perform activities such as device attestation and behavioral analysis to identify potential threats.
		Supports (example of) PM-10: Authorization Process	The ongoing device authorization service may quarantine a device, refuse a device access to the network or to certain high-value resources, or take other pre-defined action based on policy.
		Supports (example of) AC-4: Information Flow Enforcement	Behavioral analysis performed as part of ongoing device authorization may involve comparing observed activity

Logical Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			against a baseline to detect anomalies and events.
		Supports (example of) CM-2: Baseline Configuration	Behavioral analysis performed as part of ongoing device authorization may involve comparing observed activity against a baseline to detect anomalies and events in order to maintain a baseline configuration.
		Supports (example of) SI-4: System Monitoring	Device lifecycle monitoring may be used to detect attacks and indicators of potential attacks as well as anomalous security configuration changes.
		Supports (example of) CA-7: Continuous Monitoring	The ongoing device authorization service may collect and correlate data from device attestation services, behavioral analytics tools, authentication services, and other sources as input to its policy-based assessment of device authorization.
		Supports (example of) IR-4: Incident Handling	If the policy-based assessment of the device does not meet a given threshold, the device may not be authorized to access specific resources or the network itself. If the assessment of the device's trustworthiness does not meet a given threshold and, as a result, the device is denied access to the network or other resources, such restriction may help contain incidents that involve the device.

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

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

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

Table 4-6 provides a mapping between the functionality provided by the Wi-Fi Easy Connect protocol and the NIST SP 800-53 controls. This table indicates how Wi-Fi Easy Connect functions help support NIST SP 800-53 controls and vice versa.

Table 4-6 Mapping Between Wi-Fi Easy Connect Functionality and NIST SP 800-53 Controls

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Installs the device's unique private/public key pair into secure storage, either by provisioning these credentials or having them autonomously generated. Creates the device's DPP URI (i.e., the device's bootstrapping information, which includes its public key) and makes a record of devices that it has created and their associated DPP URIs.	Supports (example of) AC-6: Least Privilege	If the manufacturer installs the device's MUD URL on the device so that it can be provided to the configurator as a DPP configuration request object attribute within the Wi-Fi Easy Connect protocol, this enables the network to use the device intent information that is in the MUD file to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) CM-8: System Component Inventory	Information about the devices (e.g., device model, onboarding protocol supported, DPP URI) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	The manufacturer's factory provisioning process is responsible for ensuring that the device is provisioned with or autonomously generates its

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			own unique device credential in the form of a private/public key pair that is securely stored, as well as the DPP URI necessary for a configurator to cryptographically authenticate this device credential and then provide the device with its network-layer credential. Also, if the manufacturer provisions the device with application-layer onboarding bootstrapping information or equips the device with the capability to generate one-time application-layer bootstrapping information at runtime so that it can be provided to the configurator as a DPP configuration request object attribute within the Wi-Fi Easy Connect protocol, this enables the device to be securely provisioned with application-layer credentials as well. The device credential that is provisioned or autonomously generated during the device manufacture and provisioning process (i.e., the device's unique private/public key pair) is stored in hardware-based secure storage. Possession of this unique private key is what enables the device to have its asserted identity authenticated during onboarding.
		Is supported by (precedes) SR-3: Supply Chain Controls and Processes	The requirements that the device must meet in order to support the Wi-Fi Easy Connect protocol and meet other trusted network- and application-layer onboarding expectations of its users must be clear to the manufacturer before it creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use. For example, the device will need

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			hardware-based secure storage, Wi-Fi Easy Connect-specific firmware and software, and support for one or more types of network credentials (e.g., connector, passphrase, X.509 certificate) and may need to be provisioned with or be equipped to generate bootstrapping information it will need to support streamlined application-layer onboarding.
Supply Chain Integration Service	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information (e.g., the DPP URI) to the device owner. When using Wi-Fi Easy Connect, the device's public key, which is encoded in the DPP URI, is the device bootstrapping information that the device owner requires in order to authenticate the device, establish a secure connection to it, and proceed with the remainder of the trusted network-layer onboarding process.	Supports (precedes) CM-8: System Component Inventory	Bootstrapping information (e.g., the DPP URI) for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory so the owner will be able to authenticate the devices.
		Supports (integral to) IA-2: Identification and Authentication (Organizational Users)	The generation and transfer of device bootstrapping information (i.e., the DPP URI) from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
		Is supported by (precedes) SR-3: Supply Chain Controls and Processes	The device owner's expectations regarding the mechanism for transferring the device bootstrapping information (i.e., the DPP URI) from the manufacturer to the device owner must be made clear so the manufacturer will use the expected mechanism (e.g., direct transfer of the bootstrapping information into the device owner's database, use of a QR code encoding of the DPP URI that is imprinted on the device or its packaging, encrypted email listing device and DPP URI).
Configurator (Network-Layer	Runs the onboarding protocol to interact	Supports (integral to) AC-4: Information Flow Enforcement	The configurator authenticates the IoT device.

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
Onboarding Component)	with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information. May interact with a certificate authority to sign the certificate provided to the device as part of the device's network credentials.	Supports (example of) AC-6: Least Privilege	When the device uses the optional DPP configuration request object MUD URL attribute to securely convey its MUD URL to the configurator, the configurator supports use of the device intent information that is in the MUD file to configure ACLs on the router or switch that constrain communications to and from the device according to policy.
		Supports (integral to) AC-17: Remote Access	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The configurator is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices. Also, the provisioned credentials are unique.
		Is supported by (example of) AT-3: Role-Based Training	When using Wi-Fi Easy Connect, participation of a trusted onboarder may be required. This individual's role is to provide the device with the network's bootstrapping information and/or provide the network with the device's bootstrapping information. Before doing so, this individual is responsible for ensuring that the device is authorized to be onboarded to the network and the network is authorized to onboard the device. This trusted onboarder is not privy to any private keys held by the device or the network, but must be trusted to ensure that the device is being onboarded to the appropriate, authorized network.

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Supports (precedes) CM-8: System Component Inventory	The DPP URI for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory so the owner will be able to authenticate the devices. Bootstrapping information for all owned devices must be correlated with the device owner's inventory so that the bootstrapping information for the particular device being onboarded can be provided to the network-layer onboarding component.
		Supports (integral to) IA-3: Device Identification and Authentication	The configurator is responsible for provisioning authenticated, authorized devices with their network-layer credentials. In addition, when the device uses the DPP configuration request object to securely convey its application-layer onboarding bootstrapping information in support of streamlined application-layer onboarding (e.g., via the OCF Information configuration attribute or other optional third-party attributes), the configurator also supports the secure provisioning of application-layer credentials. Before provisioning a device with its network-layer credentials, the configurator authenticates the device using the device's bootstrapping information (i.e., its DPP URI).
		Supports (integral to) IA-4: Identifier Management	The configurator authenticates an IoT device's identity by using the device's public key to verify that the corresponding unique private key is installed on the device.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The configurator establishes an encrypted channel with the IoT device to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials,

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			device intent information, application-layer bootstrapping information).
		Is supported by (precedes) SR-3: Supply Chain Controls and Processes	The configurator of the device owner must be in possession of the device bootstrapping information (i.e., the DPP URI) in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the configurator via the device owner must be defined, well-understood, and trusted by both parties.
Access Point, Router, or Switch	Wireless access point and/or router or switch. The Wi-Fi Easy Connect protocol supports secure conveyance of the device's device intent information (e.g., the device's MUD URL) to the configurator. This MUD URL may be used by the network to configure per-device ACLs and policy when devices are onboarded.	Supports (example of) AC-6: Least Privilege	Until a device is authenticated and onboarded, the only 802.11 frames that are allowed from the device are the special pre-association action frames that are used by the Wi-Fi Easy Connect protocol. All other 802.11 frames are blocked until the device is onboarded. When a device is onboarded, device intent and other policy information for the device that is securely conveyed by the Wi-Fi Easy Connect protocol may be used to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) SC-3: Security Function Isolation	When a device is onboarded, device intent or other policy information for the device that is securely conveyed by the Wi-Fi Easy Connect protocol may be used to configure ACLs on the router in a way that essentially assigns the device to a particular network segment.
Enrollee (IoT Device)	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the Wi-Fi	Supports (example of) AC-6: Least Privilege	When the device is equipped with a MUD URL and uses the optional DPP configuration request object MUD URL attribute to securely convey this MUD URL to the configurator, the device intent information that is in the MUD file can be used to configure ACLs on

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
	Easy Connect protocol and interacts with the configurator to perform one-way or mutual authentication, establish a secure channel, and securely receive its network credentials. It may also have additional security capabilities, such as securely conveying its device intent information or its application-layer onboarding bootstrapping information (e.g., via the DPP configuration request object).		the router or switch that constrain communications to and from the device according to policy.
		Is supported by (precedes) CM-8: System Component Inventory	The organization must have an inventory of the devices that support Wi-Fi Easy Connect onboarding so it knows which devices to use in cases in which it wants to use this protocol to perform trusted network-layer onboarding. If streamlined application-layer onboarding is supported, the device must either be provisioned with its application-layer bootstrapping information prior to network-layer onboarding or have the ability to generate one-time application-layer bootstrapping information at runtime. In either case, the organization must have an inventory of the devices with these capabilities so it knows which ones to use in cases in which it wants the device to perform application-layer onboarding.
		Supports (integral to) IA-2: Device Identification and Authentication	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The IoT device establishes an encrypted channel with the configurator to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
Secure Storage	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.	Supports (integral to) IA-4: Identifier Management	The confidentiality provided to a device's private key by storing and using it in secure storage is essential to ensuring that the device's identity can be uniquely authenticated. Storing the device's network credentials in secure storage ensures their confidentiality. The device's private key, which serves as its birth credential, is installed in secure storage within the device, thereby binding the device to its credential. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) SC-12: Cryptographic Key Establishment and Management	The device's private key, which serves as its birth credential, is installed in secure storage within the device, thereby binding the device to its credential. The device may also be bound to its credential using a signed X.509 certificate.
		Supports (integral to) SC-28: Protection of Information at Rest	Information stored in secure storage is protected from unauthorized access and disclosure.
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (example of) IA-4: Identifier Management	If the network-layer credential that is provisioned is an X.509 certificate, then it will be signed by a CA and asserted by the device in order to gain access to the network. Network-layer credentials provisioned by Wi-Fi Easy Connect that are signed by a trusted CA may be verified and revoked. Note that although it is not an X.509 certificate and not related to a CA, a Wi-Fi Easy Connect connector is a signed public key. The signee is the configurator, which is trusted by all devices that are onboarded to the network. When the DPP configurator issues a connector, it signs the enrollee's protocol key to construct the connector. So the connector is a

Wi-Fi Easy Connect Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			public key signed by a trusted 3rd party (the configurator) but it is not specific to a CA.

4.2.2.2 Mapping Between BRSKI and NIST SP 800-53 Controls

Table 4-7 provides a mapping between the functionality provided by BRSKI and the NIST SP 800-53 controls. This table indicates how BRSKI functions help support NIST SP 800-53 controls and vice versa.

Table 4-7 Mapping Between BRSKI Functionality and NIST SP 800-53 Controls

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
Device Manufacture and Factory Provisioning	Manufactures the IoT device. Installs/generates the device's unique private key into secure storage and creates the associated signed 802.1AR certificate (i.e., the device's IDevID). Provides the location of the device's MASA in an extension to the IDevID. Provides the device with trust anchors for the MASA entity that will sign the returned vouchers. Installs info the device requires for application-layer onboarding (if applicable). Creates a record of devices that it has created.	Supports (example of) AC-3: Access Enforcement	When the MUD URL is provisioned to the device, information relating to device access connections can be used to manage connections.
		Supports (example of) AC-4: Information Flow Enforcement	When the MUD URL is provisioned to the device, information relating to device access connections can be used to manage connections.
		Supports (example of) AC-6: Least Privilege	If the manufacturer installs device intent information (e.g., the device's MUD URL) on the device, this information can be used by the network to configure ACLs on the router or switch to constrain communications to and from the device according to policy.
		Supports (example of) AC-17: Remote Access	When the MUD URL is provisioned to the device, information relating to device access connections can be used to manage connections.

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Supports (example of) CM-8: System Component Inventory	Information about the devices (e.g., device model, ID, onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. When the device is sold, the information will be provided to the device owner in the purchase order or other documentation. The owner may use this information as the basis of the owner's inventory information regarding devices obtained from that manufacturer.
		Supports (example of) IA-3: Device Identification and Authentication	When the MUD URL is provisioned to the device, information relating to device access connections can be used to identify the device to a network.
		Supports (integral to) IA-4: Identifier Management	The manufacturer's factory provisioning process is responsible for ensuring that the device is provisioned with or autonomously generates its own unique device credential in the form of an 802.1AR certificate (IDevID) and a private/public keypair that are securely stored so that the identity of the device can be cryptographically authenticated, and then provided with its network-layer credential. Also, if the manufacturer provisions the device with application-layer onboarding bootstrapping

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			information or equips the device with the capability to generate one-time application-layer bootstrapping information at runtime, this enables the device to be securely provisioned with application-layer credentials as well. During factory provisioning, the device's 802.1AR certificate (IDevID) is bound to its private key, which is stored in hardware-based secure storage. This credential is what enables the device to have its asserted identity authenticated during onboarding.
		Is supported by (precedes) SR-3: Supply Chain Controls and Processes	The requirements that the device must meet in order to support the BRSKI protocol and meet other trusted network- and application-layer onboarding expectations of its users must be clear to the manufacturer before it creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use. For example, the device will need hardware-based secure storage, BRSKI-specific firmware and software, and an 802.1AR certificate (e.g., connector, passphrase, X.509 certificate), and may need to

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			be provisioned with or be equipped to generate bootstrapping information it will need to support streamlined application-layer onboarding.
MASA (Supply Chain Integration Service)	The device manufacturer stores the device's serial number and IDevID in the MASA's database. When the device is sold, the manufacturer may also record the device owner information in the MASA. Storing this information in the MASA serves a mechanism whereby the device manufacturer transfers device bootstrapping information (i.e., the device's public key) to the device owner, as well as the mechanism for providing device ownership information to the device itself. The MASA consults its stored information and applies policy to determine whether or not to approve a registrar's claim that it owns a device. If so, it creates and signs a voucher that directs the device to accept its new owner and sends it back to the registrar.	Supports (precedes) CM-8: System Component Inventory	Bootstrapping information (e.g., an 802.1AR certificate) for each of the devices that the manufacturer creates must be provided to the domain registrar of the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded in the MASA in order for the device to determine whether the network is authorized to onboard the device.
		Supports (precedes) IA-3: Device Identification and Authentication	The generation and transfer of device bootstrapping information (e.g., device certificate information) from the device manufacturer to the device owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. Also, the transfer of device ownership information from the device owner to the device must occur before the device will permit itself to be onboarded to the network. The transfer of this

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			ownership and bootstrapping information is achieved by storing the device ownership information in a trusted MASA and having the MASA generate a signed voucher attesting to device ownership assertions.
		Is supported by (precedes) SR-3: Supply Chain Controls and Processes	The requirements that the device must meet in order to support the BRSKI protocol and meet other trusted network- and application-layer onboarding expectations of its users must be clear to the manufacturer before it creates and provisions the device to ensure that the device will be equipped to run the trusted network- and application-layer onboarding protocols that the owner intends to use. For example, the device will need hardware-based secure storage, BRSKI-specific firmware and software, and an 802.1AR certificate (e.g., connector, passphrase, X.509 certificate), and may need to be provisioned with or be equipped to generate bootstrapping information it will need to support streamlined application-layer onboarding. Also, the manufacturer will need to send the device ownership information to the device's trusted MASA.

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Supports (example of) SR-4: Provenance	The transfer of device ownership information from the device owner to the device must occur before the device will permit itself to be onboarded to the network. The transfer of this ownership and bootstrapping information is achieved by storing the device ownership information in a trusted MASA and having the MASA generate a signed voucher attesting to device ownership assertions.
Domain Registrar (Network-Layer Onboarding Component and Network-Layer Onboarding Authorization Service)	Runs the BRSKI onboarding protocol to interact with the IoT device and the MASA. This involves performing one-way or mutual authentication, establishing a secure channel, and securely providing local network credentials to the device. Also provides an authorization function. Prior to permitting the device to be onboarded, it examines the pledge voucher request provided by the IoT device and determines whether the device's manufacturer is known to it and whether devices of that type are welcome on the network. As part of its authorization service, it also helps the device to determine whether the network is authorized to onboard it (by serving as an intermediary for the vouchers exchanged between the device and the MASA).	Supports (integral to) AC-17: Remote Access	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The domain registrar is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices.
		Is supported by (precedes) CM-8: System Component Inventory	The certificate for each of the devices that the manufacturer creates, along with information regarding which organization owns each device is provided to the MASA. The domain registrar relies on the MASA to approve the registrar's

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			claim that it owns a device. This claim approval will be based on the fact that the MASA has been provided with a list of devices that are owned by the network. This list of device certificates constitutes an inventory of the organization's devices that must be in the MASA prior to onboarding. Bootstrapping information for all owned devices must be correlated with the device owner's inventory so that the bootstrapping information for the particular device being onboarded can be provided to the network-layer onboarding component. In addition, information regarding which entity owns a device must be recorded and available for the device to consult in order for the device to determine whether the network is authorized to onboard the device.
		Supports (integral to) IA-3: Device Identification and Authentication	The domain registrar is responsible for providing authenticated, authorized devices with a network-layer credential. The domain registrar authenticates an IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
		Supports (integral to) SC-8: Transmission	The domain registrar establishes an encrypted channel with the IoT device to ensure the confidentiality

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Confidentiality and Integrity	of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Wireless access point and/or router or switch. The router or switch may get configured with per-device ACLs and policy when devices are onboarded.	Supports (example of) AC-6: Least Privilege	When a device is onboarded, ACLs and policy for the device may be configured on the router to constrain communications to and from the device according to policy.
		Supports (example of) SC-3: Security Function Isolation	When a device is onboarded, policy for the device may be configured on the router or switch to assign the device to a particular network segment.
Pledge (IoT Device)	The IoT device that is used to demonstrate trusted network- and application-layer onboarding. It runs the onboarding protocol and interacts with the network onboarding component to perform one-way or mutual authentication, establish a secure channel, and securely request and receive its network credentials. It also interacts with the MASA via signed vouchers sent to and received from the Domain Registrar to ensure that the network that is trying to onboard it is authorized to do so before permitting itself to be onboarded.	Is supported by (precedes) CM-8: System Component Inventory	The organization must have an inventory of the devices that support BRSKI onboarding so it knows which devices to use in cases in which it wants to use this protocol to perform trusted network-layer onboarding.
		Supports (integral to) IA-3: Device Identification and Authentication	The IoT device may authenticate the network before permitting itself to be onboarded to the network. The IoT device also permits itself to be authenticated as part of the network-layer onboarding process.
		Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The IoT device establishes an encrypted channel with the domain registrar to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
Secure Storage	Storage on the IoT device that is designed to be protected from unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process the device's private key (IDevID), network credentials (LDevID), and any other information that must be kept confidential.	Supports (integral to) IA-4: Identifier Management	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to ensuring that the device's identity can be uniquely authenticated.
		Supports (integral to) SC-12: Cryptographic Key Establishment and Management	The device's private key, which serves as its birth credential along with its 802.1AR certificate (IDevID), is installed in secure storage within the device, thereby binding the device to its credential.
		Supports (integral to) SC-28: Protection of Information at Rest	Information stored in secure storage is protected from unauthorized access and disclosure.
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (integral to) AC-16: Security and Privacy Attributes	The device credential is an 802.1AR certificate (e.g., an IDevID) that is signed by a CA. This certificate binds the device's credential to the device's identity. Also, all vouchers exchanged as part of the protocol are signed, enabling claims regarding device ownership to be verified. Also, the pledge and domain registrar create and sign voucher requests using their certificates, which in turn were signed by the CA.

BRSKI Component	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		Supports (integral to) SC-12: Cryptographic Key Establishment and Management	The device credential is an 802.1AR certificate (e.g., an IDevID) that is signed by a CA. This certificate binds the device's credential to the device's identity. Also, all vouchers exchanged as part of the protocol are signed, enabling claims regarding device ownership to be verified. Also, the pledge and domain registrar create and sign voucher requests using their certificates, which in turn were signed by the CA.
		Supports (example of) SC-17: Public Key Infrastructure Certificates	Network-layer credentials provisioned by BRSKI are signed by a trusted CA, enabling them to be verified and revoked.

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. Mappings are provided only for Build 1 at this time.

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.

Table 4-8 details the mapping between the functionality provided by Build 1 components and SP 800-53 controls. It indicates how these components help support SP 800-53 controls and vice versa.

565 **Table 4-8 Mapping Between Functionality of Build 1 Components and NIST SP 800-53 Controls**

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
Supply Chain Integration Service	Aruba Central	When devices are sold, this service is the mechanism through which the device manufacturer transfers device bootstrapping information to the device owner. The manufacturer provides device bootstrapping information to the HPE Cloud via the REST API that is documented in the DPP specification. Once the device is transferred to an owner, the HPE Cloud provides the device bootstrapping information (i.e., the device's DPP URI) to the device owner's private tenancy within the HPE Cloud. Device bootstrapping information is information	Supports (precedes) AC-3: Access Enforcement	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
			Supports (precedes) AC-4: Information Flow Enforcement	Information about the device's requirements for network-layer onboarding (e.g., onboarding protocol supported) that the manufacturer creates will be recorded by the manufacturer during the factory provisioning process. Note that the generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
			Supports (integral to) CM-8: System Component Inventory	Bootstrapping information for each of the devices that the manufacturer creates must be provided to the device owner and correlated with the devices in the owner's inventory information so the owner will be able to authenticate the devices. In addition, information regarding which entity owns a device must be recorded and available for the device to

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		(e.g., a public key that pairs with the device's private key) that the device owner requires to perform trusted network-layer onboarding.		consult in order for the device to determine whether the network is authorized to onboard the device.
			Supports (example of) IA-1: Identification and Authentication Policy and Procedures	Cryptographically authenticating devices during network-layer onboarding to the device owner's network can facilitate an organization's identification and authentication policies and procedures regarding network connections to IoT devices. The network-layer credentials that are provisioned are unique to the device and can be used to identify devices on the network after onboarding has finished.
			Supports (integral to) IA-3: Device Identification and Authentication	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network.
			Supports (precedes) IA-9: Service Identification and Authentication	Device bootstrapping information is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices.
			Supports (precedes) PM-5: System Inventory	The owner of the device uses the bootstrapping information in compiling the owner's organization-wide inventory information that includes devices obtained from that manufacturer.

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			Supports (precedes) SR-4: Provenance	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. Creation, signing, and installation of the device's unique identity and other birth credentials into secure storage and creation of records of devices that the manufacturer has created support documentation and maintenance of the valid provenance of system components.
			Supports (example of) SR-5: Acquisition Strategies, Tools, and Methods	The generation and transfer of device bootstrapping information from the manufacturer to the owner must occur before the device's identity can be cryptographically authenticated during network-layer onboarding to the device owner's network. These signed device identities and records of manufactured devices can be required in acquisition and procurement documents to protect against and mitigate supply chain risks.
			Supports (example of) SR-11: Component Authenticity	During factory provisioning, the device's unique identifier is bound to its device credential (e.g., its private key) by storing the credential in hardware-based secure

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
				storage. This credential is what enables the device to have its asserted identity authenticated during onboarding. Signing and installing the device's unique identity and other birth credentials into secure storage may support implementation of anti-counterfeiting policies and procedures by providing means to detect counterfeit components and prevent them from entering the system.
			Is supported by (precedes) SR-1: Supply Chain Risk Management Policy and Procedures	The device owner's expectations regarding the mechanism for transferring the device bootstrapping information from the manufacturer to the device owner are informed by supply chain risk management policies and procedures so that the manufacturer can use expected mechanisms to enable policy enforcement (e.g., enrollment of the device's credential into a CA, direct transfer of the bootstrapping information into the device owner's database, use of a QR code that is imprinted on the device or its packaging).
Network-Layer Onboarding Component	Aruba Access Point with support from Aruba Central	Wireless access point that also serves as a router. Runs the Wi-Fi Easy Connect network-layer onboarding	Supports (integral to) AC-1: Access Control Policy and Procedures	The network-layer onboarding service supports implementation of access control policies and procedures by providing authenticated, authorized devices with a network-layer credential.

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		protocol to interact with the IoT device to perform one-way or mutual authentication, establish a secure channel, and securely provide local network credentials to the device. If the network credential that is being provided to the device is a certificate, the onboarding component will interact with a certificate authority to sign the certificate. The configurator deployed in Build 1 supports DPP 2.0, but it is also backward compatible with DPP 1.0.	Supports (integral to) AC-3: Access Enforcement	The network-layer onboarding component supports access enforcement by authenticating a connected IoT device's identity by using the device's public key to verify that the device's private key is installed on the device.
			Supports (integral to) AC-17: Remote Access	Remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely. The network-layer onboarding component is the component that is responsible for ensuring that only authenticated, authorized devices are provided with network-layer credentials, and it provides those credentials in a trusted fashion that protects their confidentiality and helps prevent them from being used by unauthorized devices. Also, the provisioned credentials are unique.
			Supports (example of) AC-19: Access Control for Mobile Devices	Where the IoT device is a mobile device, remote access is managed by ensuring that only devices that have network-layer credentials are permitted to connect to the network securely.
			Supports (integral to) AC-20: Use of External Systems	Access to the network from external systems is managed by ensuring that only devices that have network-layer credentials are permitted to connect to external systems.
			Supports (integral to) AC-24: Access Control Decisions	Access control decisions are enforced by ensuring that only devices that have network-

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
				layer credentials are permitted to connect to the network securely.
			Supports (integral to) IA-1: Identification and Authentication Policy and Procedures	The network-layer onboarding service provides a network-layer credential for authentication of authorized devices.
			Supports (integral to) IA-3: Device Identification and Authentication	The network-layer onboarding service provides a network-layer credential for authentication of authorized devices. Before provisioning a device with its network-layer credentials, the configurator authenticates the device using the device's bootstrapping information.
			Supports (precedes) IA-9: Service Identification and Authentication	Information about the device (e.g., device model, ID, onboarding protocol supported) created and provided by the manufacturer during the factory provisioning process is used to uniquely identify and authenticate necessary authorized services before establishing communications with the devices. The network-layer onboarding service supports service identification and authentication by providing a network-layer credential for authentication of authorized devices.
			Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The network-layer onboarding component establishes an encrypted channel with the IoT device to ensure the confidentiality of information

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
				they exchange (e.g., the device's network-layer credentials).
			Supports (integral to) SC-15: Collaborative Computing Devices and Applications	When a device is onboarded, ACLs and policy for the device are configured on the router to constrain communications to and from the device according to policy.
			Is supported by (precedes) CM-8: System Component Inventory	Bootstrapping information for all owned devices must be correlated with the device owner's inventory so that the bootstrapping information for the particular device being onboarded can be provided to the network-layer onboarding component.
			Is supported by (precedes) SR-1: Supply Chain Risk Management Policy and Procedures	The network-layer onboarding component of the device owner must be in possession of the device bootstrapping information in order to authenticate the device. The mechanisms by which the device bootstrapping information is conveyed from the device manufacturer to the device owner must be consistent with both manufacturer and customer supply chain risk management policies and procedures.
			Is supported by (example of) AT-3: Role-Based Training	In this build, participation of a trusted onboarder is optional. When present, this individual's role is to provide the network with the device's bootstrapping information by uploading the device's DPP URIs to a database. Before doing so, this individual is responsible for ensuring that

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
				the device is authorized to be onboarded to the network and the network is authorized to onboard the device.
			Is supported by (integral to) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the network-layer onboarding component's establishment of an encrypted channel with the IoT device in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Access Point, Router, or Switch	Aruba Access Point	Wireless access point that also serves as a router. It may get configured with per-device ACLs and policy when devices are onboarded.	Supports (example of) AC-4: Information Flow Enforcement	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment, thus enforcing approved authorizations for controlling the flow of information within the system and between connected systems based on organization-defined information flow control policies.
			Supports (example of) AC-5: Separation of Duties	When a device is onboarded, ACLs and policy for the device may be configured on the router to constrain communications to and from the device according to separation of duties policies.
			Supports (example of) AC-6: Least Privilege	When a device is onboarded, ACLs and policy for the device may be configured on the router to constrain communications to and from the device according to least privilege policies.

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			Supports (example of) AC-16: Security and Privacy Attributes	When a device is onboarded, ACLs and policy for the device may be configured on the router to constrain communications to and from the device consistent with policies regarding permitted security and privacy attributes.
			Supports (integral to) AC-17: Remote Access	When a device is onboarded, ACLs and policy for the device are configured on the router to constrain communications to and from the device.
			Supports (integral to) AC-24: Access Control Decisions	When a device is onboarded, ACLs and policy for the device are configured on the router to control decisions regarding communications to and from the device.
			Supports (example of) SC-7: Boundary Protection	When a device is onboarded, policy for the device may be configured on the router to assign the device to a particular network segment.
Network-Layer Onboarding Authorization Service	Cloud Auth (on Aruba Central)	The authorization service provides the configurator and router with the information needed to determine if the device is authorized to be onboarded to the network and, if so, whether it should be assigned any	Is supported by (precedes) CM-8: System Component Inventory	An inventory of IoT devices belonging to the network owner must be available for the network-layer onboarding authorization service to consult in order for it to determine whether or not the device is authorized to be onboarded to the network.

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
		special roles or be subject to any specific access controls. It provides device authorization, role-based access control, and policy enforcement.		
Build-Specific IoT Device	Aruba UXI Sensor	The IoT device that is used to demonstrate both trusted network-layer onboarding and trusted application-layer onboarding. It runs the Wi-Fi Easy Connect network-layer onboarding protocol supported by the build to securely receive its network credentials. It also has an application that enables it to perform independent application-layer onboarding.	Supports (integral to) IA-3: Device Identification and Authentication	The IoT device permits itself to be authenticated as part of the network-layer onboarding process.
			Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials). If application-layer onboarding is also supported, the IoT device establishes an encrypted channel with the application-layer service to ensure confidentiality of information exchanged (e.g., the device's application-layer credentials).
			Is supported by (precedes) CM-8: System Component Inventory	To support UXI application-layer onboarding, the device must have been provisioned with its application-layer bootstrapping information and software prior to network-layer onboarding. The organization must have an inventory of the devices with this UXI application-layer onboarding capability so it

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
				knows which devices to use in cases in which it wants the device to perform application-layer onboarding
			Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Generic IoT Device	Raspberry Pi	The IoT device that is used to demonstrate only trusted network-layer onboarding.	Supports (integral to) IA-3: Device Identification and Authentication	The IoT device permits itself to be authenticated as part of the network-layer onboarding process.
			Supports (integral to) SC-8: Transmission Confidentiality and Integrity	The IoT device establishes an encrypted channel with the network-layer onboarding component to ensure the confidentiality of all information they exchange (e.g., the device's network-layer credentials).
			Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Secure Storage	Aruba UXI Sensor Trusted Platform	Storage on the IoT device that is designed to be protected from	Supports (integral to) AC-1: Access Control Policy and Procedures	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to implementation

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
	Module (TPM)	unauthorized access and capable of detecting attempts to tamper with its contents. Used to store and process private keys, credentials, and other information that must be kept confidential.		of the organization's access control policy.
			Supports (integral to) IA-1: Policy and Procedures	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to the effective implementation of the organization's identification and authentication policies as they relate to IoT.
			Supports (integral to) AC-3: Access Enforcement	The secure storage of the device's private key, which serves as its birth credential within the device and binds the device to its credential, is an essential element of the access enforcement mechanism.
			Supports (integral to) IA-3: Device Identification and Authentication	The confidentiality provided to a device's private key and credentials by storing and using them in secure storage is essential to the effectiveness and security of device identification and authentication processes. The device may also be bound to its credential using a signed X.509 certificate.
			Supports (integral to) SC-28: Protection of Information at Rest	Information stored in secure storage is protected from unauthorized access and disclosure.
			Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
				(e.g., the device's network-layer credentials).
Certificate Authority (CA)	Private CA	Issues and signs certificates as needed.	Supports (integral to) IA-3: Device Identification and Authentication	If the device's network-layer credential is an X.509 certificate (e.g., an LDevID) that is signed by a trusted CA, this certificate binds the device's credential to the device's identity. It provides a mechanism for enabling the credential to be verified and revoked that is essential to the integrity of the authentication process.
			Is supported by (precedes) SC-12: Cryptographic Key Establishment and Management	Secure establishment and management of cryptographic keys is a prerequisite for the IoT device's establishment of an encrypted channel with the network-layer onboarding component in order to ensure the confidentiality of information they exchange (e.g., the device's network-layer credentials).
Application-Layer Onboarding Service	UXI Application and UXI Cloud	After connecting to the network, the device downloads its application-layer credentials from the UXI cloud and uses these to authenticate to the UXI application, with which it interacts.	Supports (example of) AC-18: Wireless Access	The application-layer onboarding component may establish a wireless encrypted channel with the IoT device to ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
			Supports (integral to) IA-3: Device Identification and Authentication	The application-layer onboarding service is responsible for providing authenticated, authorized devices with an application-layer credential.
			Supports (integral to) SC-8: Transmission	The application-layer onboarding component establishes an encrypted channel with the IoT device to

Build 1 Architecture Component	Product	Component's Function	Function's Relationships to SP 800-53 Controls	Relationship Explanation
			Confidentiality and Integrity	ensure the confidentiality of all information they exchange (e.g., the device's application-layer credentials).
			Is supported by (precedes) CM-8: System Component Inventory	To support UXI application-layer onboarding, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the manufacturer will create an inventory of the devices that have been provisioned for each application service.

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] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,* National Institute of Standards and Technology, Gaithersburg, MD, April 2018, 48 pp. Available: https://doi.org/10.6028/NIST.CSWP.04162018

[3] 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

[4] Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Gaithersburg, MD, September 2020, 465 pp. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[5] 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

[6] NIST Risk Management Framework. Available: https://csrc.nist.gov/projects/risk-management/about-rmf