

**NIST SPECIAL PUBLICATION 1800-36C**

---

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

## Enhancing Internet Protocol-Based IoT Device and Network Security

---

**Volume C:  
How-To Guides**

**Murugiah Souppaya  
Paul Watrobski**

National Institute of Standards and Technology  
Gaithersburg, Maryland

**Chelsea Deane  
Joshua Klosterman  
Blaine Mulugeta  
Charlie Rearick  
Susan Symington**

The MITRE Corporation  
McLean, Virginia

**Dan Harkins  
Danny Jump**

Aruba, a Hewlett Packard  
Enterprise company  
San Jose, California

**Andy Dolan  
Kyle Haefner  
Craig Pratt  
Darshak Thakore**

CableLabs  
Louisville, Colorado

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>



## 1 **DISCLAIMER**

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

8 While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk  
9 through outreach and application of standards and best practices, it is the stakeholder’s responsibility to  
10 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise,  
11 and the impact should the threat be realized before adopting cybersecurity measures such as this  
12 recommendation.

13 National Institute of Standards and Technology Special Publication 1800-36C, Natl. Inst. Stand. Technol.  
14 Spec. Publ. 1800-36C, 33 pages, October 2023, CODEN: NSPUE2

## 15 **FEEDBACK**

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

18 Comments on this publication may be submitted to: [iot-onboarding@nist.gov](mailto:iot-onboarding@nist.gov).

19 Public comment period: October 31, 2023 through December 15, 2023

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

21 National Cybersecurity Center of Excellence  
22 National Institute of Standards and Technology  
23 100 Bureau Drive  
24 Mailstop 2002  
25 Gaithersburg, MD 20899  
26 Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

## 27 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

28 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards  
29 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and  
30 academic institutions work together to address businesses' most pressing cybersecurity issues. This  
31 public-private partnership enables the creation of practical cybersecurity solutions for specific  
32 industries, as well as for broad, cross-sector technology challenges. Through consortia under  
33 Cooperative Research and Development Agreements (CRADAs), including technology partners—from  
34 Fortune 50 market leaders to smaller companies specializing in information technology security—the  
35 NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity  
36 solutions using commercially available technology. The NCCoE documents these example solutions in  
37 the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework  
38 and details the steps needed for another entity to re-create the example solution. The NCCoE was  
39 established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,  
40 Maryland.

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

## 43 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 53 **KEYWORDS**

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

56 **ACKNOWLEDGMENTS**

57 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
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
Loic Cavaille	NXP Semiconductors
Mihai Chelalau	NXP Semiconductors

Name	Organization
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
Karen Scarfone	Scarfone Cybersecurity
Steve Clark	SEALSQ, a subsidiary of WISeKey
Pedro Fuentes	SEALSQ, a subsidiary of WISeKey
Gweltas Radenac	SEALSQ, a subsidiary of WISeKey
Kalvin Yang	SEALSQ, a subsidiary of WISeKey
Mike Dow	Silicon Labs
Steve Egerter	Silicon Labs

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

62 **Technology Collaborators**

- |  |                                    |  |
|--|------------------------------------|--|
| 63 <a href="#">Aruba</a> , a Hewlett Packard | <a href="#">Foundries.io</a>       | <a href="#">Open Connectivity Foundation (OCF)</a> |
| 64 Enterprise company                        | <a href="#">Kudelski IoT</a>       | <a href="#">Sandelman Software Works</a>           |
| 65 <a href="#">CableLabs</a>                 | <a href="#">NquiringMinds</a>      | <a href="#">SEALSQ</a> , a subsidiary of WISeKey   |
| 66 <a href="#">Cisco</a>                     | <a href="#">NXP Semiconductors</a> | <a href="#">Silicon Labs</a>                       |

67 **DOCUMENT CONVENTIONS**

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

75 **CALL FOR PATENT CLAIMS**

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

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

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

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

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

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

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

100 Such statements should be addressed to: [iot-onboarding@nist.gov](mailto:iot-onboarding@nist.gov).

101 **Contents**

102 **1 Introduction .....1**

103 1.1 How to Use This Guide ..... 1

104 1.2 Build Overview ..... 3

105 1.2.1 Reference Architecture Summary ..... 3

106 1.2.2 Physical Architecture Summary..... 3

107 1.3 Typographic Conventions ..... 6

108 **2 Build 1 (Wi-Fi Easy Connect, Aruba/HPE) .....7**

109 2.1 Aruba Central/Hewlett Packard Enterprise (HPE) Cloud ..... 7

110 2.2 Aruba Wireless Access Point ..... 7

111 2.2.1 Wi-Fi Network Setup/Configuration..... 8

112 2.2.2 Wi-Fi Easy Connect Configuration ..... 9

113 2.3 Cisco Catalyst 3850-S Switch ..... 9

114 2.3.1 Configuration ..... 10

115 2.4 Aruba User Experience Insight (UXI) Sensor ..... 10

116 2.4.1 Configuration ..... 10

117 2.5 Raspberry Pi..... 10

118 2.5.1 Configuration ..... 11

119 2.5.2 DPP Onboarding ..... 11

120 2.6 Certificate Authority..... 13

121 2.6.1 Private Certificate Authority..... 13

122 2.6.2 SEALSQ INeS..... 17

123 2.7 UXI Cloud ..... 18

124 **3 Build 2 (Wi-Fi Easy Connect, CableLabs, OCF) .....18**

125 3.1 CableLabs Platform Controller ..... 18

126 3.1.1 Operation/Demonstration..... 18

127 3.2 CableLabs Custom Connectivity Gateway ..... 19

128 3.2.1 Installation/Configuration ..... 19

129 3.2.2 Integration with CableLabs Platform Controller ..... 19

130 3.2.3 Operation/Demonstration..... 19

131 3.3 Reference Clients/IoT Devices..... 19

132 3.3.1 Installation/Configuration ..... 19

133            3.3.2    Operation/Demonstration..... 19

134 **4    Build 3 (BRSKI, Sandelman Software Works) .....20**

135        4.1    Onboarding Router/Join Proxy..... 20

136            4.1.1    Setup and Configuration..... 20

137        4.2    Minerva Join Registrar Coordinator ..... 20

138            4.2.1    Setup and Configuration..... 20

139        4.3    Reach Pledge Simulator..... 21

140            4.3.1    Setup and Configuration..... 21

141        4.4    Serial Console Server ..... 22

142        4.5    Minerva Highway MASA Server ..... 22

143            4.5.1    Setup and Configuration..... 23

144        4.6    IoT Devices..... 23

145            4.6.1    Setup/Installation ..... 23

146        4.7    SEALSQ Certificate Authority..... 23

147 **5    Build 4 (Thread, Silicon Labs, Kudelski IoT) .....23**

148 **6    Build 5 (BRSKI, NquiringMinds) .....23**

149 **7    Factory Provisioning Builds .....23**

150 **Appendix A    List of Acronyms .....24**

151 **Appendix B    References .....25**

152 **List of Figures**

153 **Figure 1-1 NCCoE IoT Onboarding Laboratory Physical Architecture.....5**

## 154 1 Introduction

155 The following volumes of this guide show information technology (IT) professionals and security  
156 engineers how we implemented these example solutions. We cover all of the products employed in this  
157 reference design. We do not re-create the product manufacturers' documentation, which is presumed  
158 to be widely available. Rather, these volumes show how we incorporated the products together in our  
159 environment.

160 *Note: These are not comprehensive tutorials. There are many possible service and security configurations*  
161 *for these products that are out of scope for this reference design.*

### 162 1.1 How to Use This Guide

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

172 NIST is adopting an agile process to publish this content. Each volume is being made available as soon as  
173 possible rather than delaying release until all volumes are completed. Work continues on implementing  
174 the example solutions and developing other parts of the content. As a preliminary draft, we will publish  
175 at least one additional draft for public comment before it is finalized.

176 This guide contains five volumes:

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

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

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

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

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

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

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

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

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

227 A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a  
228 preliminary draft guide. As the project progresses, this preliminary draft will be updated. We seek

229 feedback on the publication’s contents and welcome your input. Comments, suggestions, and success  
230 stories will improve subsequent versions of this guide. Please contribute your thoughts to [iot-  
onboarding@nist.gov](mailto:iot-<br/>231 onboarding@nist.gov).

## 232 1.2 Build Overview

233 This NIST Cybersecurity Practice Guide addresses the challenge of network-layer onboarding using  
234 standards-based protocols to perform trusted network-layer onboarding of an IoT device. Each build  
235 demonstrates one or more of these capabilities:

- 236       ▪ Trusted Network-Layer Onboarding: providing the device with its unique network credentials  
237       over an encrypted channel
- 238       ▪ Network Re-Onboarding: performing trusted network-layer onboarding of the device again,  
239       after device reset
- 240       ▪ Network Segmentation: assigning a device to a segment of the network
- 241       ▪ Trusted Application-Layer Onboarding: providing the device with application-layer credentials  
242       over an encrypted channel after completing network-layer onboarding
- 243       ▪ Ongoing Device Authorization: continuously monitoring the device on an ongoing basis,  
244       providing policy-based assurance and authorization checks on the device throughout its lifecycle

245 Currently, five builds that will serve as examples of how to onboard IoT devices using the protocols  
246 described in NIST SP 1800-36B, as well as the factory provisioning builds, are being implemented and  
247 will be demonstrated as part of this project. The remainder of this practice guide provides step-by-step  
248 instructions on how to reproduce the three builds that have been completed so far: Builds 1 (Wi-Fi Easy  
249 Connect, Aruba/HPE), 2 (Wi-Fi Easy Connect, CableLabs, OCF), and 3 (BRSKI, Sandelman Software  
250 Works). Step-by-step instructions for Builds 4 (Thread, Silicon Labs, Kudelski IoT), 5 (BRSKI,  
251 NquiringMinds), and the factory provisioning builds will be included in future updates to this document.

### 252 1.2.1 Reference Architecture Summary

253 The builds described in this document are instantiations of the trusted network-layer onboarding and  
254 lifecycle management logical reference architecture that is described in NIST SP 1800-36B. This  
255 architecture is organized according to five high-level processes: Device Manufacture and Factory  
256 Provisioning, Device Ownership and Bootstrapping Information Transfer, Trusted Network-Layer  
257 Onboarding, Trusted Application-Layer Onboarding, and Continuous Assurance. For a full explanation of  
258 the architecture, please see NIST SP 1800-36B: *Approach, Architecture, and Security Characteristics*.

### 259 1.2.2 Physical Architecture Summary

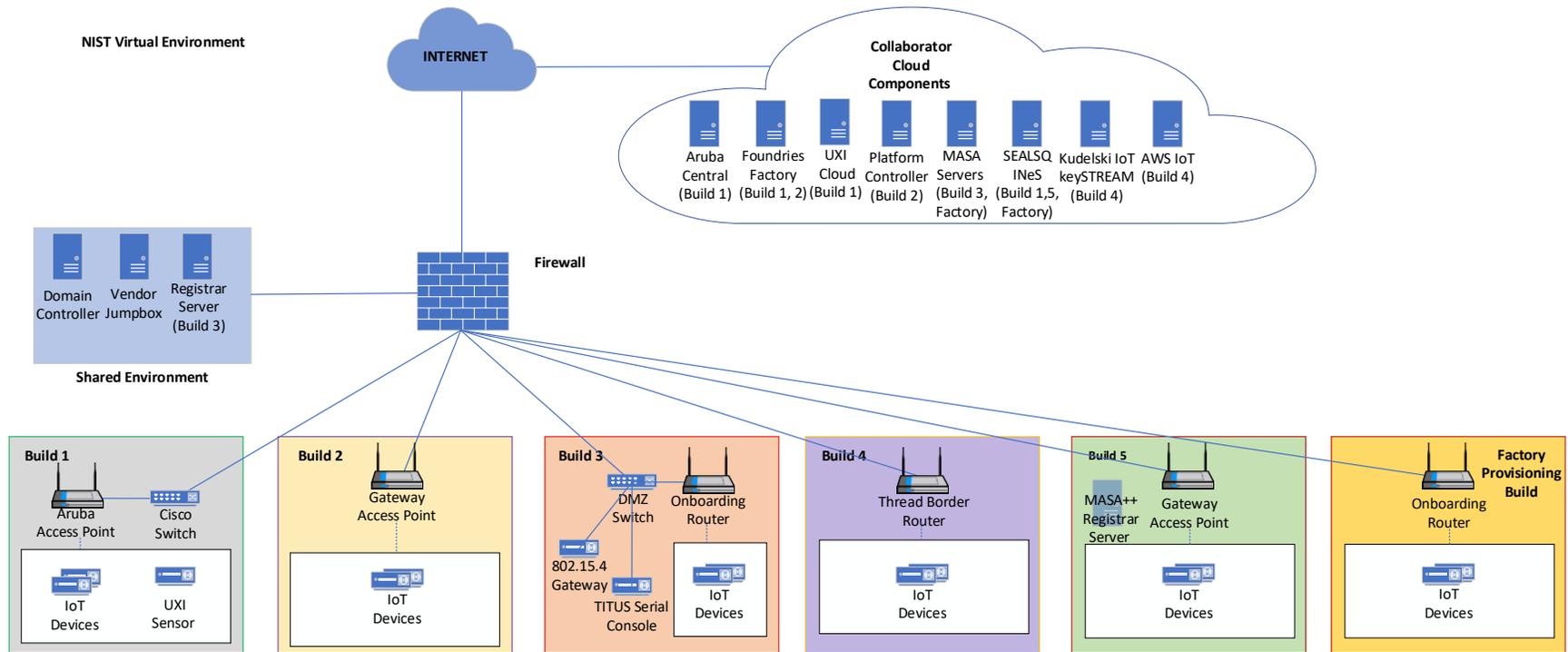
260 [Figure 1-1](#) depicts the high-level physical architecture of the NCCoE IoT Onboarding laboratory  
261 environment in which the five trusted IoT device network-layer onboarding project builds and the two  
262 factory provisioning builds are being implemented. The NCCoE provides virtual machine (VM) resources  
263 and physical infrastructure for the IoT Onboarding lab. As depicted, the NCCoE IoT Onboarding  
264 laboratory hosts collaborator hardware and software for the builds. The NCCoE also provides  
265 connectivity from the IoT Onboarding lab to the NIST Data Center, which provides connectivity to the

266 internet and public IP spaces (both IPv4 and IPv6). Access to and from the NCCoE network is protected  
267 by a firewall.

268 Access to and from the IoT Onboarding lab is protected by a pfSense firewall, represented by the brick  
269 box icon in [Figure 1-1](#). This firewall has both IPv4 and IPv6 (dual stack) configured. The IoT Onboarding  
270 lab network infrastructure includes a shared virtual environment that houses a domain controller and a  
271 vendor jumpbox. These components are used across builds where applicable. It also contains five  
272 independent virtual local area networks (VLANs), each of which houses a different trusted network-layer  
273 onboarding build.

274 The IoT Onboarding laboratory network has access to cloud components and services provided by the  
275 collaborators, all of which are available via the internet. These components and services include Aruba  
276 Central and the User Experience Insight (UXI) Cloud (Build 1), Platform Controller (Build 2), a  
277 Manufacturer Authorized Signing Authority (MASA) server (Builds 3, 5), Kudelski IoT keySTREAM  
278 application-layer onboarding service and Amazon Web Services (AWS) IoT (Build 4), and  
279 FoundriesFactory and SEALSQ INeS, which we anticipate will be used across numerous builds.

280 Figure 1-1 NCCoE IoT Onboarding Laboratory Physical Architecture



281 All six network-layer onboarding laboratory environments, as depicted in the diagram, have been  
282 installed:

- 283       ▪ The Build 1 network infrastructure within the NCCoE lab consists of two components: the Aruba  
284       Access Point and the Cisco Switch. Build 1 also requires support from Aruba Central for network-  
285       layer onboarding and the UXI Cloud for application-layer onboarding. These components are in  
286       the cloud and accessed via the internet. The IoT devices that are onboarded using Build 1  
287       include the UXI Sensor and the Raspberry Pi.
- 288       ▪ The Build 2 network infrastructure within the NCCoE lab consists of a single component: the  
289       Gateway Access Point. Build 2 also requires support from the Platform Controller, which also  
290       hosts the IoTivity Cloud Service. The IoT devices that are onboarded using Build 2 include three  
291       Raspberry Pis.
- 292       ▪ The Build 3 network infrastructure components within the NCCoE lab include a Wi-Fi capable  
293       home router (including Join Proxy), a DMZ switch (for management), and an ESP32A Xtensa  
294       board acting as a Wi-Fi IoT device, as well as an nRF52840 board acting as an IEEE 802.15.4  
295       device. A management system on a BeagleBone Green acts as a serial console. A registrar server  
296       has been deployed as a virtual appliance on the NCCoE private cloud system. Build 3 also  
297       requires support from a MASA server which is accessed via the internet. In addition, a Raspberry  
298       Pi provides an ethernet/802.15.4 gateway, as well as a test platform.
- 299       ▪ The Build 4 network infrastructure components within the NCCoE lab include an Open Thread  
300       Border Router, which is implemented using a Raspberry Pi, and a Silicon Labs Gecko Wireless  
301       Starter Kit, which acts as an 802.15.4 antenna. Build 4 also requires support from the Kudelski  
302       IoT keySTREAM service, which is in the cloud and accessed via the internet. The IoT device that  
303       is onboarded in Build 4 is the Silicon Labs Thunderboard (BRD2601A) with an EFR32MG24  
304       System-on-Chip. The application service to which it onboards is AWS IoT.
- 305       ▪ The Build 5 network infrastructure components within the NCCoE lab include an OpenWRT  
306       router, a Turris Omnia Wi-Fi access point, the MASA++ Registration Server, and a USB hub. This  
307       build leverages the NquiringMinds' cloud service called tdx Volt in conjunction with the RADIUS  
308       service that resides on the router to provide authentication capabilities for network-layer  
309       onboarding to take place. The IoT device that is onboarded using Build 5 is a Feather HUZAH  
310       ESP8266.
- 311       ▪ The factory provisioning build network infrastructure partially shares the Wi-Fi capable home  
312       router with Build 3 for network-layer onboarding. The IoT devices in this build are Raspberry Pis  
313       equipped with a SEALSQ VaultIC Secure Element, which is provisioned credentials in  
314       coordination with the cloud-based SEALSQ INES Certificate Authority. The factory provisioning  
315       build also includes a cloud-based MASA server to support BRSKI capabilities.

316 The remainder of this guide will focus on the setup and configuration of Builds 1, 2, and 3. Information  
317 for Builds 4, 5, and the factory provisioning builds are planned for future updates to this document.

### 318 **1.3 Typographic Conventions**

319 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<code>service sshd start</code>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a> .

## 320 2 Build 1 (Wi-Fi Easy Connect, Aruba/HPE)

321 This section of the practice guide contains detailed instructions for installing and configuring all the  
 322 products used to build an instance of the example solution. For additional details on Build 1's logical and  
 323 physical architectures, see NIST SP 1800-36B: *Approach, Architecture, and Security Characteristics*.

324 The network-layer onboarding component of Build 1 utilizes Wi-Fi Easy Connect, also known as the  
 325 Device Provisioning Protocol (DPP). The Wi-Fi Easy Connect standard is maintained by the Wi-Fi Alliance  
 326 [4]. The term "DPP" is used when referring to the network-layer onboarding protocol, and "Wi-Fi Easy  
 327 Connect" is used when referring to the overall implementation of the network onboarding process.

### 328 2.1 Aruba Central/Hewlett Packard Enterprise (HPE) Cloud

329 This build utilized Aruba Central as a cloud management service that provided management and support  
 330 for the Aruba Wireless Access Point (AP) and provided authorization and DPP onboarding capabilities for  
 331 the wireless network. A cloud-based application programming interface (API) endpoint provided the  
 332 ability to import the DPP Uniform Resource Identifiers (URIs) in the manner of a Supply Chain  
 333 Integration Service. Due to this capability and Build 1's support for Wi-Fi Easy Connect, Build 1's  
 334 infrastructure fully supported interoperable network-layer onboarding with Build 2's Reference Clients  
 335 ("IoT devices") provided by CableLabs.

### 336 2.2 Aruba Wireless Access Point

337 Use of DPP is implicitly dependent on the Aruba Central cloud service. Aruba Central provides a cloud  
 338 Infrastructure as a Service (IaaS) enabled architecture that includes initial support for DPP in Central  
 339 2.5.6/ArubaOS (AOS) 10.4.0. Central and AOS support multiple deployment formats:

- 340 1. As AP only, referred to as an *underlay deployment*, where traffic is bridged locally from the APs.
- 341 2. An *overlay deployment*, where all data is securely tunneled to an on-prem gateway where  
 342 advanced services can route, inspect, and analyze the data before it's either bridged locally or  
 343 routed to its next hop.

344 3. A *mixed-mode deployment*, which is a combination of the two where a returned 'role/label' is  
345 used to determine how the data is processed and forwarded.

346 At the time of this publication, a user can leverage any 3xx, 5xx, or 6xx APs to support a DPP  
347 deployment, with a view that all future series APs will implicitly include support. For an existing or new  
348 user there is a prerequisite of the creation of a Service Set Identifier (SSID). Note that DPP today is not  
349 supported under Wi-Fi Protected Access 3 (WPA3); this is a roadmap item with no published timeline.

350 Assuming there is an existing SSID or a new one is created based upon the above security restrictions,  
351 the next step is to enable DPP (as detailed below in [Section 2.2.1](#)) such that the SSID can support  
352 multiple authentication and key managements (AKMs) on a Basic Service Set (BSS). If the chosen security  
353 type is DPP, only a single AKM will exist for that BSS.

354 A standards-compliant 802.3at port is the easiest method for providing the AP with power. An external  
355 power supply can also be used.

356 Within this document, we do not cover the specifics of radio frequency (RF) design and placement of  
357 APs. Guidance and assistance is available within the Aruba community site,  
358 <https://community.arubanetworks.com> or the Aruba Support Portal, <https://asp.arubanetworks.com>.  
359 Additionally, we do not cover onboarding and licensing of Aruba Central hardware. Documentation can  
360 be found here: <https://www.arubanetworks.com/techdocs/ArubaDocPortal/content/docportal.htm>.

### 361 2.2.1 Wi-Fi Network Setup/Configuration

362 The following instructions detail the initial setup and configuration of the Wi-Fi network upon powering  
363 on and connecting the AP to an existing network.

- 364 1. Navigate to the Aruba Central cloud management interface.
- 365 2. On the sidebar, navigate under **Global** and choose the AP-Group you want to configure/modify.  
366 (This assumes you have already grouped your APs by location/functions.)
- 367 3. Under **Devices**, click on **Config** in the top right side.
- 368 4. You will now be in the Access Points tab and WLANs tab. Do one of the following:
  - 369 a. If creating a new SSID, click on **+ Add SSID**. After entering the Name (SSID) in Step 1 and  
370 configuring options as necessary in Step 2, when you get to Step 3 (Security), it will  
371 default on the slide-bar to the Personal Security Level; the alternative is the Enterprise  
372 Security Level.
    - 373 i. If you choose the **Personal Security Level**, under **Key-Management** ensure you  
374 select either **DPP** or **WPA2-Personal**. If you choose **WPA2-Personal**, expand the  
375 **Advanced Settings** section and enable the toggle button for DPP so that the SSID  
376 can broadcast the AKM. Note that this option is not available if choosing DPP for  
377 Key-Management.
    - 378 ii. If you choose the **Enterprise Security Level**, only WPA2-Enterprise Key-  
379 Management currently supports DPP. Expand the **Advanced Settings** section and  
380 enable the toggle button for **DPP** so that the SSID can broadcast the AKM.

- 381                   b. If you plan to enable DPP on a previously created SSID:
- 382                    i. Ensure you are running version 10.4+ on your devices. You also need an SSID that
- 383                    is configured for WPA2-Personal or WPA2-Enterprise.
- 384                    ii. When ready, float your cursor over the previously created SSID name you wish to
- 385                    configure and click on the edit icon.
- 386                    iii. Edit the SSID, click on **Security**, and expand the **Advanced Settings** section and
- 387                    enable the toggle button for **DPP**.
- 388                    iv. Click **Save Settings**.

389 For SSIDs that have been modified to add DPP AKM, it's also necessary to enable DPP within the radio

390 profile.

- 391           1. Under the **Access Point** Tab, click on **Radios**.
- 392           2. It's expected you'll see a **default** radio-profile. If a custom one has been created, you'll need to
- 393           review your configuration before proceeding.
- 394           3. Assuming a **default** radio-profile, click on the **Edit** icon, expand **Show advanced settings**, and
- 395           scroll down to **DPP Provisioning**. You can selectively enable this for 2.4 GHz or 5.0 GHz. Support
- 396           for DPP on 6.0 GHz is a roadmap item at this time and is not yet available.

## 397 2.2.2 Wi-Fi Easy Connect Configuration

398 Configuration of the Access Point occurred through the Aruba Central cloud management interface.

399 Standard configurations were used to stand up the Build 1 wireless network. The instructions for

400 enabling DPP capabilities for the overall wireless network are listed below:

- 401           1. Navigate to the Aruba Central cloud management interface.
- 402           2. On the sidebar, navigate to **Security > Authentication and Policy > Config**.
- 403           3. In the **Client Access Policy** section, click **Edit**.
- 404           4. Under the **Wi-Fi Easy Connect™ Service** heading, ensure that the name of your wireless network
- 405           is selected.
- 406           5. Click **Save**.

## 407 2.3 Cisco Catalyst 3850-S Switch

408 This build utilized a Cisco Catalyst 3850-S switch. This switch utilized a minimal configuration with two

409 separate VLANs to allow for IoT device network segmentation and access control. The switch also

410 provided Power-over-Ethernet support for the Aruba Wireless AP.

### 411 2.3.1 Configuration

412 The switch was configured with two VLANs, and a trunk port dedicated to the Aruba Wireless AP. You  
413 can find the relevant portions of the Cisco iOS configuration below:

```
414 interface Vlan1
415     no ip address
416 interface Vlan2
417     no ip address
418 interface GigabitEthernet1/0/1
419     switchport mode trunk
420 interface GigabitEthernet1/0/2
421     switchport mode access
422     switchport access vlan 1
423 interface GigabitEthernet1/0/3
424     switchport mode access
425     switchport access vlan 2
```

## 426 2.4 Aruba User Experience Insight (UXI) Sensor

427 This build utilized an Aruba UXI Sensor as a Wi-Fi Easy Connect-capable IoT device. Models G6 and G6C  
428 support Wi-Fi Easy Connect, and all available G6 and G6C models support Wi-Fi Easy Connect within  
429 their software image. This sensor successfully utilized the network-layer onboarding mechanism  
430 provided by the wireless network and completed onboarding to the application-layer UXI cloud service.  
431 The network-layer onboarding process is automatically initiated by the device on boot.

### 432 2.4.1 Configuration

433 All of Aruba's available G6 and G6C UXI sensors support the ability to complete network-layer and  
434 application-layer onboarding. No specific configuration of the physical sensor is required. As part of the  
435 supply-chain process, the cryptographic public key for your sensor(s) will be available within the cloud  
436 tenant. This public/private keypair for each device is created as part of the manufacturing process. The  
437 public key effectively identifies the sensor to the network and as part of the Wi-Fi Easy Connect/DPP  
438 onboarding process. This allows unprovisioned devices straight from the factory to be onboarded and  
439 subsequently connect to the UXI sensor cloud to obtain their network-layer configuration. An  
440 administrator will have to define the 'tasks' the UXI sensor is going to perform such as monitoring SSIDs,  
441 performing reachability tests to on-prem or cloud services, and making the results of these tests  
442 available within the UXI user/administrator portal.

## 443 2.5 Raspberry Pi

444 In this build, the Raspberry Pi 3B+ acts as a DPP enrollee. In setting up the device for this build, a DPP-  
445 capable wireless adapter, the Alfa AWUS036NHA network dongle, was connected to enable the Pi to  
446 send and receive DPP frames. Once fully configured, the Pi can onboard with the Aruba AP.

## 447 2.5.1 Configuration

448 The following steps were completed for the Raspberry Pi to complete DPP onboarding:

- 449 1. Set the management IP for the Raspberry Pi to an IP address in the Build 1 network. To do this,  
450 add the following lines to the file *dhcpcd.conf* located at */etc/dhcpcd.conf*. For this build, the IP  
451 address was set to 192.168.10.3.

```
# Example static IP configuration:  
interface eth0  
static ip_address=192.168.10.3/24  
#static ip6_address=fd51:42f8:caae:d92e::ff/64  
static routers=192.168.10.1  
static domain_name_servers=192.168.10.1 8.8.8.8
```

- 452 2. Install Linux Libraries using the apt package manager. The following packages were installed:

- 453 a. autotools-dev
- 454 b. automake
- 455 c. libcurl4-openssl-dev
- 456 d. libnl-genl-3-dev
- 457 e. libavahi-client-dev
- 458 f. libavahi-core-dev
- 459 g. aircrack-ng
- 460 h. openssl-1.1.1q

- 461 3. Install the DPP utilities. These utilities were installed from the GitHub repository  
462 <https://github.com/HewlettPackard/dpp> using the following command:

```
463 git clone https://github.com/HewlettPackard/dpp
```

## 464 2.5.2 DPP Onboarding

465 This section describes the steps for using the Raspberry Pi as a DPP enrollee. The Pi uses a DPP utility to  
466 send out chirps to make its presence known to available DPP configurators. Once the Pi is discovered,  
467 the DPP configurator (Aruba Wireless AP) initiates the DPP authentication protocol. During this phase,  
468 DPP *connectors* are created to onboard the device to the network. As soon as the Pi is fully  
469 authenticated, it is fully enrolled and can begin normal network communication.

- 470 1. Navigate to the DPP utilities directory which was installed during setup:

```
471 cd dpp/linux
```

- 472 2. From the DPP utilities directory, run the following command to initiate a DPP connection:

```
473 sudo ./sss -I wlan1 -r -e sta -k resp256.pem -B respbkeys.txt -a -t -d 255
```

```

build1@Build1Pi:~/dpp/linux $ sudo ./sss -I wlan1 -r -e sta -k resp256.pem -B respbkeys.txt -a -t -d 255
adding interface wlan1...
wlan1 is NOT the loopback!

getting the interface!
got phy info!!!
interface MAC address is 00:c0:ca:98:42:37
wiphy is 1
wlan1 is interface 4 from ioctl
wlan1 is interface 4 from if_nameindex()
max ROC is 5000
got driver capabilities, off chan is ok, max_roc is 5000

ask for GAS request frames

ask for GAS response frames

ask for GAS comeback request frames

ask for GAS comeback response frames

ask for DPP action frames
socket 4 is for nl_sock_in
role: enrollee
interfaces and MAC addresses:
    wlan1: 00:c0:ca:98:42:37
chirping, so scan for APs
scanning for all SSIDs
scan finished.
didn't find the DPP Configurator connectivity IE on
FOUND THE DPP CONFIGURATOR CONNECTIVITY IE on Build1-IoTOnboarding, on frequency 2462, channel 11

```

- 474      3. Once the enrollee has found a DPP configurator, the DPP authentication protocol is initiated.

```

----- Start of DPP Authentication Protocol -----
chirp list:
    2437
    2412
    2462
start chirping...
error...-95: Unspecific failure
changing frequency to 2437
sending 68 byte frame on 2437
chirp on 2437...
error...-95: Unspecific failure
changing frequency to 2412
sending 68 byte frame on 2412
chirp on 2412...
error...-95: Unspecific failure
changing frequency to 2462
sending 68 byte frame on 2462
chirp on 2462...
processing 222 byte incoming management frame
enter process_dpp_auth_frame() for peer 1
    peer 1 is in state DPP bootstrapped
Got a DPP Auth Frame! In state DPP bootstrapped
type Responder Bootstrap Hash, length 32, value:
05d54478 eaa59dfa 768d8148 f119f729 060c8d3b b9e917dc 4b34d654 32f403cb

type Initiator Bootstrap Hash, length 32, value:
2795ec93 1b5b17c9 e0e5e5ad b2ce787d 413ab0c2 bb29cfbf 554668fe a090eeee

type Initiator Protocol Key, length 64, value:
bbb37f18 0839880d 7d5bb455 c6702cde fe51d0ee 2c93b895 0edb368d 23d9eca1
d8fc9568 c7af6542 e97aeeb4 bbae7885 05745f8d 82cac4c5 376cc6fb 30d956af

type Protocol Version, length 1, value:
02

type Wrapped Data, length 41, value:
62ceb78b 1b27d2d0 726b9f12 918736a3 ba0d8c68 00ab1509 9e2ebbc5 e61250fe
b90fc9e3 0e97cd5b b6

responder received DPP Auth Request
peer sent a version of 2
Pi'
x:
bbb37f18 0839880d 7d5bb455 c6702cde fe51d0ee 2c93b895 0edb368d 23d9eca1
y:
d8fc9568 c7af6542 e97aeeb4 bbae7885 05745f8d 82cac4c5 376cc6fb 30d956af
k1:
8de1c000 01b44e44 dbaf5bd5 273f4621 bb33bd6f f48e1dc1 3db71ba2 8852d293

initiator's nonce:
378708d9 2985f2a6 239e7ffa 0ee1649a

initiator role: configurator
my role: enrollee

```

## 475 2.6 Certificate Authority

476 The function of the certificate authority (CA) in this build is to issue network credentials for use in the  
477 network-layer onboarding process.

### 478 2.6.1 Private Certificate Authority

479 A private CA was provided as a part of the DPP demonstration utilities in the HPE GitHub repository. For  
480 demonstration purposes, the Raspberry Pi is used as the configurator and the enrollee.

481 

### 2.6.1.1 Installation/Configuration

482 The following instructions detail the initial setup and configuration of the private CA using the DPP  
 483 demonstration utilities and certificates located at <https://github.com/HewlettPackard/dpp>.

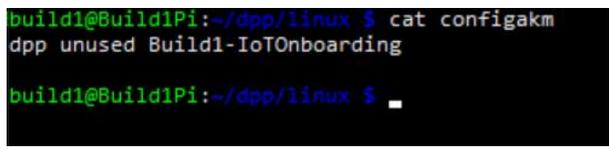
- 484 1. Navigate to the DPP utilities directory on the Raspberry Pi: `~/dpp/linux`

485 `cd dpp/linux/`

- 486 2. The README in the GitHub repository  
 487 (<https://github.com/HewlettPackard/dpp/blob/master/README>) references a text file called  
 488 `configakm` which contains information about the network policies for a configurator to provision  
 489 on an enrollee. The format is: `<akm> <EAP server> <ssid>`. Current AKMs that are supported  
 490 are DPP, dot1x, sae, and psk. For this build, DPP is used. For DPP, an Extensible Authentication  
 491 Protocol (EAP) server is not used.

- 492 3. Configure the file `configakm` located in `~/dpp/linux/`. This file instructs the configurator on how  
 493 to deploy a DPP connector (network credential) from the configurator to the enrollee. As shown  
 494 below, the `configakm` file is filled with the following fields:

495 `dpp unused Build1-IoTOnboarding.`



```
build1@Build1Pi:~/dpp/linux $ cat configakm
dpp unused Build1-IoTOnboarding

build1@Build1Pi:~/dpp/linux $
```

- 496 4. The file `csrattrs.conf` contains attributes to construct an Abstract Syntax Notation One (ASN.1)  
 497 string. This string allows the configurator to tell the enrollee how to generate a certificate  
 498 signing request (CSR). The following fields were used for this demonstration:

499 `asn1 = SEQUENCE: seq_section`

500 `[seq_section]`

501 `field1 = OID:challengePassword`

502 `field2 = SEQUENCE:ecattrs`

503 `field3 = SEQUENCE:extnd`

504 `field4 = OID:ecdsa-with-SHA256`

505 `[ecattrs]`

506 `field1 = OID:id-ecPublicKey`

507 `field2 = SET:curve`

508 `[curve]`

509 `field1 = OID:prime256v1`

```

510     [extnd]
511     field1 = OID:extReq
512     field2 = SET:extattrs

513     [extattrs]
514     field1 = OID:serialNumber
515     field2 = OID:favouriteDrink

```

```

asn1 = SEQUENCE:seq_section
[seq_section]
field1 = OID:challengePassword
field2 = SEQUENCE:ecatrs
field3 = SEQUENCE:extnd
field4 = OID:ecdsa-with-SHA256

[ecatrs]
field1 = OID:id-ecPublicKey
field2 = SET:curve

[curve]
field1 = OID:prime256v1

[extnd]
field1 = OID:extReq
field2 = SET:extattrs

[extattrs]
field1 = OID:serialNumber
field2 = OID:favouriteDrink

```

### 516 *2.6.1.2 Operation/Demonstration*

517 Once setup and configuration have been completed, the following steps can be used to demonstrate  
518 utilizing the private CA to issue credentials to a requesting device.

- 519 1. Open three terminals on the Raspberry Pi: one to start the certificate program, one to show the  
520 configurator's point of view, and one to show the enrollee's point of view.
- 521 2. The demonstration uses an OpenSSL certificate. To run the program from the first terminal,  
522 navigate to the following directory: `~/dpp/ecca/`, and run the command: `./ecca`.

```

build1@Build1Pi:~/dpp/ecca $ ./ecca
not sending my cert with p7
_

```

- 523 3. On the second terminal, start the configurator using the following command:

```

524 sudo ./sss -I lo -r -c signp256.pem -k resp256.pem -B respbkeys.txt -d 255

```

```

build1@Build1Pi:~/App/linux $ sudo ./sss -I lo -r -c signp256.pem -k resp256.pem -B respbkeys.txt -d 255
[sudo] password for build1:
adding interface lo...
role: configurator
AKM: dpp, auxdata: unused, SSID: Build1-IoTonboarding
interfaces and MAC addresses:
    lo: b8:9d:1c:2e:82:35
configured channel 2437
we are not the initiator, version is 1
my private bootstrap key:
0bd4de71 b0001946 ddc1d011 4e0ddb2 0b1ae219 915db220 6e7470fb cfcf9721

my public bootstrap key
x:
cb87856e 544a055e eb97ab88 72eb08f2 0ee36ea2 fc5fc7e5 75070dba a69a9ae2

y:
95020fc7 965def6c ebf10337 ab2850ca 2f370eb9 3d02d1ac fb9d977c be0f8f

DER encoded ASN.1:
3039301306072a8648ce3d020106082a8648ce3d03010703220003cb87856e544a055e eb97ab8872eb08f20ee36ea2fc5fc7e575070dbaa69a9ae2

----- Start of DPP Authentication Protocol -----

```

525 As shown in the terminal where the ecca program is running, the configurator contacts the CA  
526 and asks for the certificate.

```

build1@Build1Pi:~/dpp/ecca $ ./ecca
not sending my cert with p7
got a new request!
adding 4 to the service context
DER-encoded CA cert in a P7 is 517 bytes
b64-encoded message is 703 bytes

said message is 703
write 703 message

```

527 4. On the third terminal, start the enrollee using the following command:  
528 `sudo ./sss -I lo -r -e sta -k initp256.pem -B initbkeys.txt -t -a -q -d 255`  
529 From the enrollee's perspective, it will send chirps on different channels until it finds the  
530 configurator. Once found, it sends its certificate to the CA for signing. The snippet below is of  
531 the enrollee generating the CSR.

```

authenticated initiator!
start the configuration protocol...
exit process_dpp_auth_frame() for peer 1
    peer 1 is in state DPP authenticated
beginning DPP Config protocol
sending a GAS_INITIAL_REQUEST dpp config frame
processing 198 byte incoming management frame
got a GAS_INITIAL_RESPONSE...
response len is 155, comeback delay is 0
got a DPP config response!
Configurator said we need a CSR to continue...
CSR Attributes:
4d457747 43537147 53496233 4451454a 427a4156 42676371 686b6a4f 50514942
4d516f47 43437147 534d3439 41774548 4d423447 43537147 53496233 4451454a
0a446a45 5242674e 56424155 4743676d 534a6f6d 54386978 6b415155 47434371
47534d34 3942414d 430a

adding 88 byte challengePassword
an object, not an attribute
a nid for challengePassword
CSR Attr parse: got a SET OF attributes... nid for ecPublicKey
    an elliptic curve, nid = 415
CSR Attr parse: got a SET OF attributes... an extension request:
    for serial number
    for favorite drink
an object, not an attribute
a nid for ecdsa with sha256
using bootstrapping key for CSR...
CSR is 537 chars:

```

- 532 5. In the ecca terminal, the certificate from the enrollee is shown

```

Write out database with 1 new entries
Data Base Updated
DER-encoded P7 is 681 bytes
b64-encoded message is 923 bytes

said message is 923
write 923 message

```

## 533 2.6.2 SEALSQ INeS

534 The SEALSQ INeS Certificate Management System provides CA and certificate management capabilities  
535 for Build 1. Implementation of this system provides Build 1 with a trusted, public CA to support issuing  
536 network credentials.

### 537 2.6.2.1 Setup and Configuration

538 To support this build, a custom software agent was deployed on a Raspberry Pi in the Build 1 network.  
539 This agent interacted with the cloud-based CA in SEALSQ INeS via API to sign network credentials.  
540 Network-level onboarding of IoT devices was completed via DPP, with network credentials being  
541 successfully requested from and issued by SEALSQ INeS.

542 Additional information on interacting with the SEALSQ INeS API can be found at  
543 <https://inesdev.certifyiddemo.com/>. Access can be requested directly from SEALSQ via their contact  
544 form: <https://www.sealsq.com/contact>.

## 545 2.7 UXI Cloud

546 The UXI Cloud is a web-based application that serves as a monitoring hub for the UXI sensor. It provides  
547 visibility into the data captured by the performance monitoring that the UXI sensor conducts. For the  
548 purposes of this build, the dashboard was used to demonstrate application-layer onboarding, which  
549 occurs once the UXI sensor has completed network-layer onboarding. Once application-layer  
550 onboarding was completed and the application configuration had been applied to the device, our  
551 demonstration concluded.

## 552 3 Build 2 (Wi-Fi Easy Connect, CableLabs, OCF)

553 This section of the practice guide contains detailed instructions for installing and configuring all of the  
554 products used to build an instance of the example solution. For additional details on Build 2's logical and  
555 physical architectures, see NIST SP 1800-36B: *Approach, Architecture, and Security Characteristics*.

556 The network-layer onboarding component of Build 2 utilizes Wi-Fi Easy Connect, also known as the  
557 Device Provisioning Protocol (DPP). The Wi-Fi Easy Connect standard is maintained by the Wi-Fi Alliance  
558 [4]. The term "DPP" is used when referring to the network-layer onboarding protocol, and "Wi-Fi Easy  
559 Connect" is used when referring to the overall implementation of the network onboarding process.

### 560 3.1 CableLabs Platform Controller

561 The CableLabs Platform Controller provides an architecture and reference implementation of a cloud-  
562 based service that provides management capability for service deployment groups, access points with  
563 the deployment groups, registration and lifecycle of user services, and the secure onboarding and  
564 lifecycle management of users' Wi-Fi devices. The controller also exposes APIs for integration with third-  
565 party systems for the purpose of integrating various business flows (e.g., integration with manufacturing  
566 process for device management).

567 The Platform Controller would typically be hosted by the network operator or a third-party service  
568 provider. It can be accessed via web interface. Additional information for this deployment can be  
569 accessed at the official CableLabs repository:  
570 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-release/docs/Ref-AP-Setup-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Ref-AP-Setup-for-NCCoE/nccoe-ap-setup.md)  
571 [for-NCCoE/nccoe-ap-setup.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Ref-AP-Setup-for-NCCoE/nccoe-ap-setup.md).

#### 572 3.1.1 Operation/Demonstration

573 Once configuration of the Platform Controller, Gateway, and Reference Client has been completed, full  
574 operation can commence. Instructions for this are located at the official CableLabs repository:  
575 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md)  
576 [release/docs/Raspberry\\_Pi\\_Deployment.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md).

## 577 **3.2 CableLabs Custom Connectivity Gateway**

578 In this deployment, the gateway software is running on a Raspberry Pi 3B+, which acts as a router,  
579 firewall, wireless access point, Open Connectivity Foundation (OCF) Diplomat, and OCF Onboarding Tool.  
580 The gateway is also connected to the CableLabs Platform Controller, which manages much of the  
581 configuration and functions of the gateway. Due to Build 2's infrastructure and support of Wi-Fi Easy  
582 Connect, Build 2 fully supported interoperable network-layer onboarding with Build 1's IoT devices.

### 583 **3.2.1 Installation/Configuration**

584 Hardware requirements, pre-installation steps, installation steps, and configuration instructions for the  
585 gateway can be found at the official CableLabs repository:

586 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-release/docs/Ref-AP-Setup-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Ref-AP-Setup-for-NCCoE/nccoe-ap-setup.md)  
587 [for-NCCoE/nccoe-ap-setup.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Ref-AP-Setup-for-NCCoE/nccoe-ap-setup.md).

### 588 **3.2.2 Integration with CableLabs Platform Controller**

589 Once initial configuration has occurred, the gateway can be integrated with the CableLabs Platform  
590 Controller. Instructions can be found at the official CableLabs repository:

591 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-release/docs/Ref-AP-Setup-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Ref-AP-Setup-for-NCCoE/nccoe-ap-setup.md)  
592 [for-NCCoE/nccoe-ap-setup.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Ref-AP-Setup-for-NCCoE/nccoe-ap-setup.md)

### 593 **3.2.3 Operation/Demonstration**

594 Once configuration of the Platform Controller, Gateway, and Reference Client has been completed, full  
595 operation can commence. Instructions for this are located at the official CableLabs repository:

596 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md)  
597 [release/docs/Raspberry\\_Pi\\_Deployment.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md).

## 598 **3.3 Reference Clients/IoT Devices**

599 Three reference clients were deployed in this build, each on a Raspberry Pi 3B+. They were each  
600 configured to emulate either a smart light switch or a smart lamp. The software deployed also included  
601 the capability to perform network-layer onboarding via Wi-Fi Easy Connect/DPP and application-layer  
602 onboarding using the OCF onboarding method. These reference clients were fully interoperable with  
603 network-layer onboarding to Build 1.

### 604 **3.3.1 Installation/Configuration**

605 Hardware requirements, pre-installation, installation, and configuration steps for the reference clients  
606 are detailed in the official CableLabs repository:

607 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md)  
608 [release/docs/Raspberry\\_Pi\\_Deployment.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md).

### 609 **3.3.2 Operation/Demonstration**

610 Once configuration of the Platform Controller, Gateway, and Reference Client has been completed, full  
611 operation can commence. Instructions for this are located at the official CableLabs repository:

612 [https://github.com/cablelabs/Streamlined\\_Onboarding\\_Demo/blob/nccoe-](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-)  
613 [release/docs/Raspberry\\_Pi\\_Deployment.md](https://github.com/cablelabs/Streamlined_Onboarding_Demo/blob/nccoe-release/docs/Raspberry_Pi_Deployment.md).

614 For interoperability with Build 1, the IoT device's DPP URI was provided to Aruba Central, which allowed  
615 Build 1 to successfully complete network-layer onboarding with the Build 2 IoT devices.

## 616 **4 Build 3 (BRSKI, Sandelman Software Works)**

617 This section of the practice guide contains detailed instructions for installing and configuring all of the  
618 products used to build an instance of the example solution. For additional details on Build 3's logical and  
619 physical architectures, see NIST SP 1800-36B: *Approach, Architecture, and Security Characteristics*.

620 The network-layer onboarding component of Build 3 utilizes the Bootstrapping Remote Secure  
621 Infrastructure (BRSKI) protocol. Build 3 is representative of a typical home or small office network.

### 622 **4.1 Onboarding Router/Join Proxy**

623 The onboarding router quarantines the IoT device attempting to join the network until the BRSKI  
624 onboarding process is complete. The router in this build is a Turris MOX device, which is based on the  
625 Linux OpenWrt version 4 operating system (OS). The Raspberry Pi 3 contains software to function as the  
626 Join Proxy for the pledges to the network. If another brand of device is used, a different source of  
627 compiled Join Proxy might be required.

#### 628 **4.1.1 Setup and Configuration**

629 The router needs to be IPv6 enabled. In the current implementation, the join package operates on an  
630 unencrypted network, but this will be updated in a future version of the build.

### 631 **4.2 Minerva Join Registrar Coordinator**

632 The purpose of the Join Registrar is to determine whether a new device is allowed to join the network.  
633 The Join Registrar is located on a virtual machine running Devuan Linux 4 within the network.

#### 634 **4.2.1 Setup and Configuration**

635 The Minerva Fountain Join Registrar/Coordinator is available as a Docker container and as a VM in OVA  
636 format at: <https://minerva.sandelman.ca/fountain/>. Further setup and configuration instructions are  
637 available on the Sandelman website: <https://minerva.sandelman.ca/fountain/configuration/>.

638 For the Build 3 demonstration, the VM deployment was installed onto a VMware vSphere system.

639 A freshly booted VM image will do the following on its own:

- 640     ▪ Configure a database
- 641     ▪ Configure a local certificate authority (fountain:s0\\_setup\\_jrc)
- 642     ▪ Configure certificates for the database connection
- 643     ▪ Configure certificates for the Registrar https interface
- 644     ▪ Configure certificates for use with the Bucardo database replication system

- 645       ▪ Configure certificates for LDevID certification authority (fountain:s2\\_create\\_registrar)
- 646       ▪ Start the JRC

647 The root user is permitted to log in on the console ("tty0") using the password "root" but is immediately  
648 forced to set a new password.

649 The new registrar will announce itself with the name minerva-fountain.local in mDNS.

650 The logs for this are put into `/var/log/configure-fountain-12345.log` (where 12345 is a new number  
651 based upon the PID of the script).

## 652 4.3 Reach Pledge Simulator

653 The Reach Pledge Simulator acts as an IoT device in Build 3. The pledge is acting as an IoT device joining  
654 the network and is hosted on a Raspberry Pi 3. More information is available on the Sandelman website:  
655 <https://minerva.sandelman.ca/reach/>.

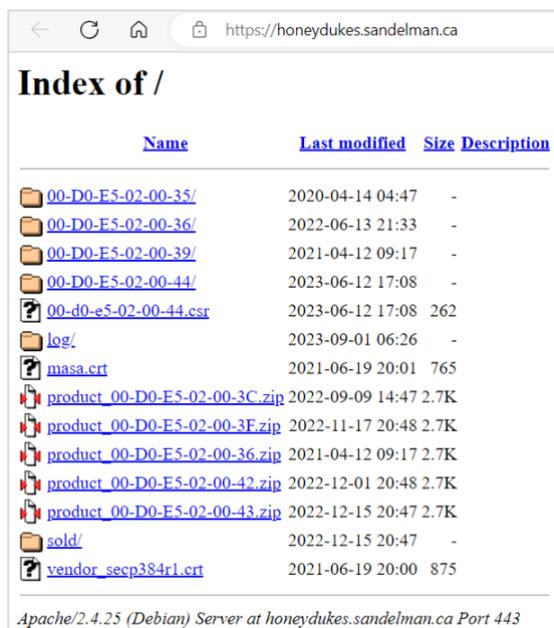
### 656 4.3.1 Setup and Configuration

657 While the functionality of this device is to act as an IoT device, it runs on the same software as the Join  
658 Registrar Coordinator. This software is available in both VM and Docker container format. Please see  
659 [Section 4.2.1](#) for installation instructions.

660 When setting up the Reach Pledge Simulator, the address of the Join Registrar Coordinator is  
661 automatically determined by the pledge.

662 Currently, the Reach Pledge Simulator obtains its IDevID using the following steps:

- 663       1. View the available packages by visiting <https://honeydukes.sandelman.ca>.



- 664       2. Open a terminal on the Raspberry Pi device and navigate to the Reach directory by entering:

665 `cd reach`

```
nccoe@satine:~$ ls
bin minerva reach
nccoe@satine:~$ cd reach
nccoe@satine:~/reach$
```

666 3. Enter the following command while substituting the URL for one of the available zip files  
667 containing the IDevID of choice on <https://honeydukes.sandelman.ca>.

668 `wget https://honeydukes.sandelman.ca/product_00-D0-E5-02-00-42.zip`

```
nccoe@satine:~/reach$ wget https://honeydukes.sandelman.ca/product_00-D0-E5-02-00-42.zip
--2023-09-01 15:49:54-- https://honeydukes.sandelman.ca/product_00-D0-E5-02-00-42.zip
Resolving honeydukes.sandelman.ca (honeydukes.sandelman.ca)... 2a01:7e00:e000:2bb::3d:b021, 176.58.120.209
Connecting to honeydukes.sandelman.ca (honeydukes.sandelman.ca)|2a01:7e00:e000:2bb::3d:b021|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2722 (2.7K) [application/zip]
Saving to: 'product_00-D0-E5-02-00-42.zip'

product_00-D0-E5-02-00-42.zip 100%[=====>] 2.66K --KB/s in 0.001s
2023-09-01 15:49:57 (3.27 MB/s) - 'product_00-D0-E5-02-00-42.zip' saved [2722/2722]
```

669 4. Unzip the file by entering the following command, substituting the name of your zip file (the  
670 IDevID is the *device.crt* file):

671 `unzip product_00-D0-E5-02-00-42.zip`

```
nccoe@satine:~/reach$ unzip product_00-D0-E5-02-00-42.zip
Archive: product_00-D0-E5-02-00-42.zip
  creating: 00-D0-E5-02-00-42/
  inflating: 00-D0-E5-02-00-42/device.crt
  inflating: 00-D0-E5-02-00-42/masa.crt
  inflating: 00-D0-E5-02-00-42/vendor.crt
  inflating: 00-D0-E5-02-00-42/key.pem
```

672 In a future implementation of the build, the IDevID will be obtained using the SEALSQ INeS Certificate  
673 Management Service.

## 674 4.4 Serial Console Server

675 The serial console server does not participate in the onboarding process but provides direct console  
676 access to the IoT devices. The serial console server has been attached to a multi-port USB hub and USB  
677 connectors and/or USB2TTL adapters connected to each device. The ESP32 and the nRF52840 are both  
678 connected to the serial console and receive power from the USB hub. Power to the console and IoT  
679 devices is also provided via the USB hub. A BeagleBone Green device was used as the serial console,  
680 using the "screen" program as the telecom device.

## 681 4.5 Minerva Highway MASA Server

682 In the current implementation of the build, the MASA server provides the Reach Pledge Simulator with  
683 an IDevID Certificate and a public/private keypair. In a future version of this build, the public/private  
684 keypair will be generated by the SEALSQ INeS Certificate Management Service.

#### 685 4.5.1 Setup and Configuration

686 Installation of the Minerva Highway MASA is described at  
687 <https://minerva.sandelman.ca/highway/configuration/>. Additional configuration details are available at  
688 <https://minerva.sandelman.ca/openssl/2022/06/10/configuring-highway-development.html>.

689 Availability of VMs and containers is described at  
690 <https://minerva.sandelman.ca/containers/2018/11/14/minerva-lxd-update.html>.

### 691 4.6 IoT Devices

692 In the current implementation of the build, onboarding of the IoT devices has not yet been  
693 implemented. Currently, the Reach Pledge Simulator is being utilized to simulate an IoT device joining  
694 the network.

#### 695 4.6.1 Setup/Installation

696 The IoT devices need to be provisioned with an IDevID. In a future version of this build, the IDevID will  
697 be provisioned using the SEALSQ INeS Certificate Management System.

### 698 4.7 SEALSQ Certificate Authority

699 The SEALSQ INeS Certificate Management System provides CA and certificate management capabilities  
700 for Build 3. Implementation of this system will provide Build 3 with a trusted, public CA to support  
701 issuing network credentials. This collaboration is in progress and will be described in a future version of  
702 this document.

## 703 5 Build 4 (Thread, Silicon Labs, Kudelski IoT)

704 In future releases of this practice guide, this section will contain detailed instructions for installing and  
705 configuring all of the products used to build an instance of the example solution.

## 706 6 Build 5 (BRSKI, NquiringMinds)

707 In future releases of this practice guide, this section will contain detailed instructions for installing and  
708 configuring all of the products used to build an instance of the example solution.

## 709 7 Factory Provisioning Builds

710 In future releases of this practice guide, this section will contain detailed instructions for installing and  
711 configuring all of the products used to build an instance of the example solution.

**712 Appendix A List of Acronyms**

<b>AKM</b>	Authentication and Key Management
<b>AOS</b>	ArubaOS
<b>AP</b>	Access Point
<b>API</b>	Application Programming Interface
<b>ASN.1</b>	Abstract Syntax Notation One
<b>AWS</b>	Amazon Web Services
<b>BSS</b>	Basic Service Set
<b>CA</b>	Certificate Authority
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>CSR</b>	Certificate Signing Request
<b>DMZ</b>	Demilitarized Zone
<b>DPP</b>	Device Provisioning Protocol (Wi-Fi Easy Connect)
<b>EAP</b>	Extensible Authentication Protocol
<b>HPE</b>	Hewlett Packard Enterprise
<b>IaaS</b>	Infrastructure as a Service
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IoT</b>	Internet of Things
<b>IPv4</b>	Internet Protocol Version 4
<b>IPv6</b>	Internet Protocol Version 6
<b>MASA</b>	Manufacturer Authorized Signing Authority
<b>MUD</b>	Manufacturer Usage Description
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>OCF</b>	Open Connectivity Foundation
<b>OS</b>	Operating System
<b>RF</b>	Radio Frequency
<b>SP</b>	Special Publication
<b>SSID</b>	Service Set Identifier

<b>URI</b>	Uniform Resource Identifier
<b>USB</b>	Universal Serial Bus
<b>UXI</b>	User Experience Insight
<b>VLAN</b>	Virtual Local Area Network
<b>VM</b>	Virtual Machine
<b>WLAN</b>	Wireless Local Area Network
<b>WPA2</b>	Wi-Fi Protected Access 2
<b>WPA3</b>	Wi-Fi Protected Access 3

713 **Appendix B**    **References**

714 [1]    Wi-Fi Alliance. *Wi-Fi Easy Connect*. Available: <https://www.wi-fi.org/discover-wi-fi/wi-fi-easy->  
715    [connect](https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect).