Trusted IoT Device Onboarding Taxonomy

IETF IoTOPS Working Group Interim Meeting

Paul Watrobski, NIST/NCCoE

Susan Symington, The MITRE Corporation/NCCoE

April 20, 2021

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- Background
- Drivers
- NIST Cybersecurity Paper: Trusted IoT Device Network-Layer Onboarding and Lifecycle Management Paper (Draft)
- Onboarding overview and concepts
- National Cybersecurity Center of Excellence (NCCoE) IoT Onboarding Project

Background

In support of the NCCoE project on trusted IoT device onboarding

- Developed with input from stakeholders

Not a submission for adoption for the IETF, but…

- If you find this work useful, please use it
- We want to be aligned, so please let us know if you perceive conflicts

Drivers

Trusted network layer onboarding is crucial for

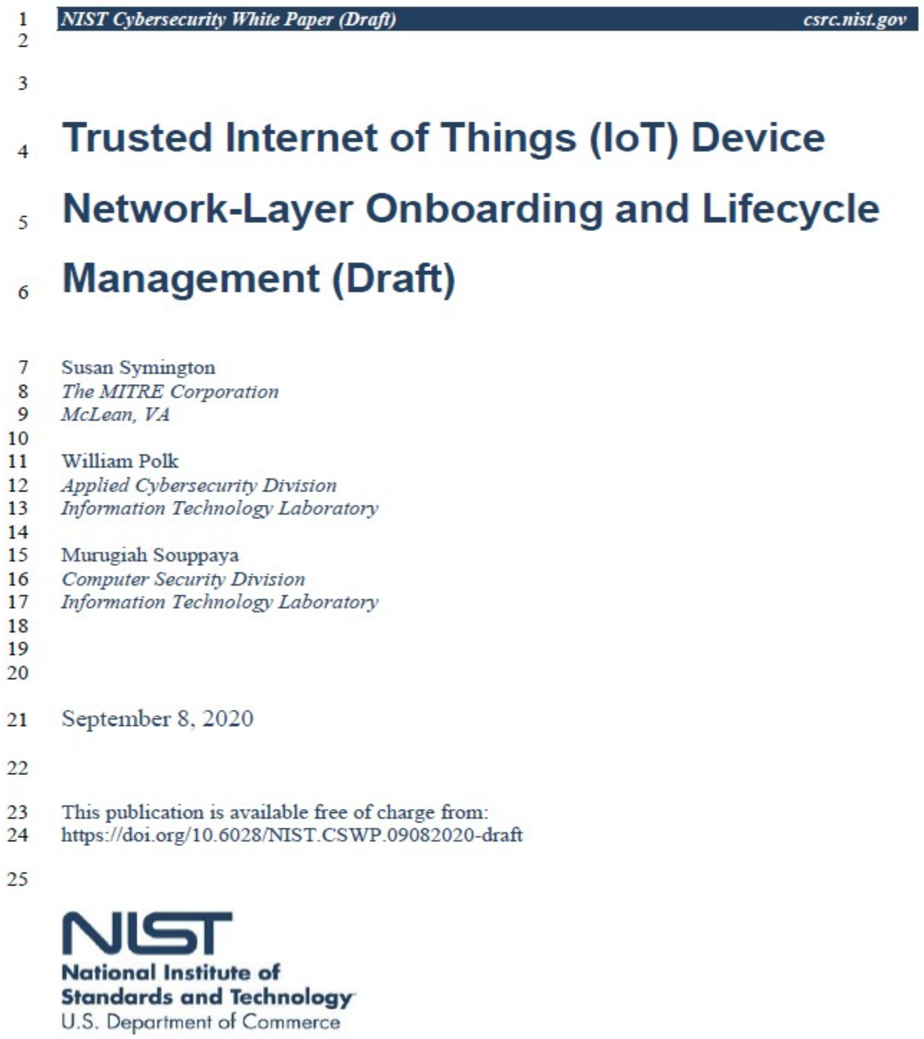
- Protecting IoT devices from being taken over by unauthorized networks
- Protecting networks from having unauthorized devices connect
- It can also enhance additional security capabilities that protect the IoT device on an ongoing basis throughout its lifecycle

Onboarding solutions have various characteristics and capabilities

A consistent taxonomy is needed to

- Clearly describe and classify the properties of any particular onboarding solution
- Express onboarding requirements and related responsibilities and processes
- Assist with discussion, characterization, and development of onboarding solutions

NIST Cybersecurity Paper



NIST Cybersecurity White Paper (Draft) *csrc.nist.gov*

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

Susan Symington
The MITRE Corporation
McLean, VA

William Polk
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

September 8, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.09082020-draft

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

- Describes a generic onboarding process and functional roles
- Onboarding lifecycle management
- Taxonomy of onboarding solution characteristics (product-agnostic)
  - User, manufacturer, and service provider perspectives
  - Consumer vs. enterprise
  - No sector-specific requirements
- Recommended security capabilities

DRAFT NIST CSWP, Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management

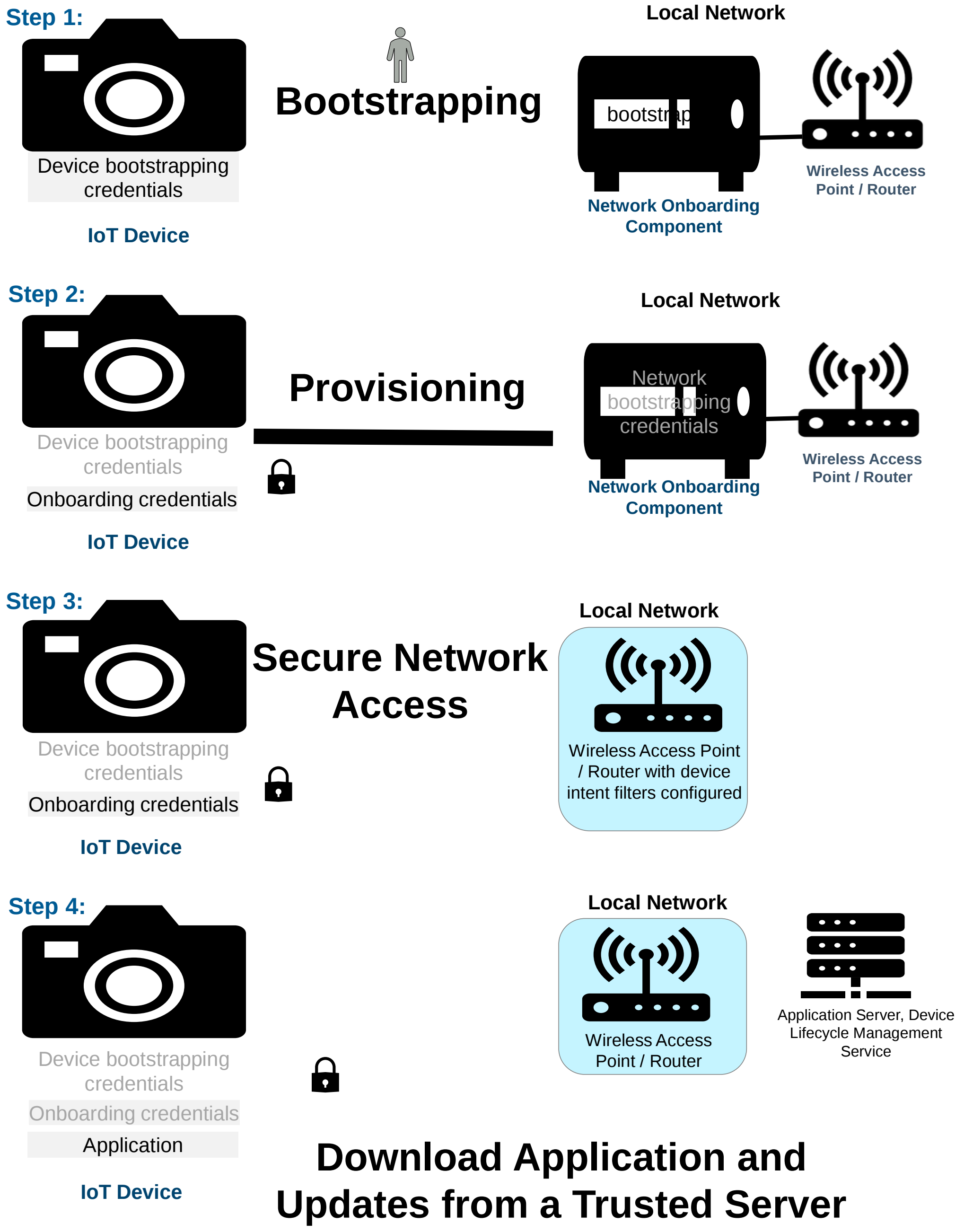
Onboarding Overview

Network-Layer Onboarding

- Provision a device with its network credentials
  - Bootstrapping: Establish trust, set up a secure channel with *network onboarding component*
  - Provisioning: Provide *onboarding credentials* to the device

Application-Layer Onboarding

- Provision a device with application-layer components
  - Performed automatically after secure connection
- Analogous to network-layer onboarding
  - Bootstrapping: establish trust, set up a secure channel between with application servers
  - Provisioning: Securely download applications, updates, and configurations to the device



Step 1:

Device bootstrapping credentials

IoT Device

Bootstrapping

Local Network

bootstrap

Network Onboarding Component

Wireless Access Point / Router

Step 2:

Device bootstrapping credentials

Onboarding credentials

IoT Device

Provisioning

Local Network

Network bootstrapping credentials

Network Onboarding Component

Wireless Access Point / Router

Step 3:

Device bootstrapping credentials

Onboarding credentials

IoT Device

Secure Network Access

Local Network

Wireless Access Point / Router with device intent filters configured

Step 4:

Device bootstrapping credentials

Onboarding credentials

Application

IoT Device

Local Network

Wireless Access Point / Router

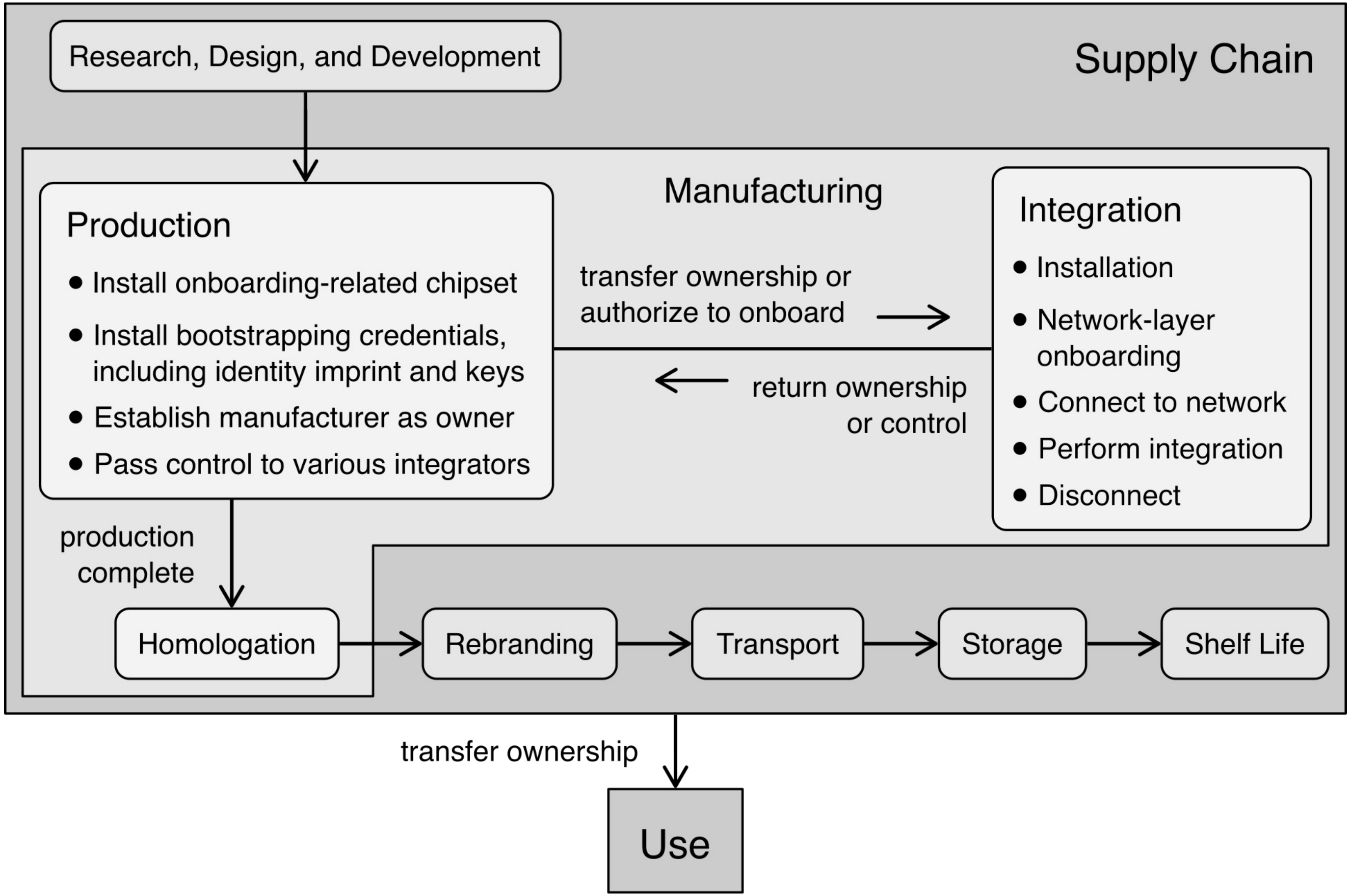
Application Server, Device Lifecycle Management Service

Download Application and Updates from a Trusted Server

Onboarding-Related Aspects of Lifecycle Management (Supply Chain Phase)

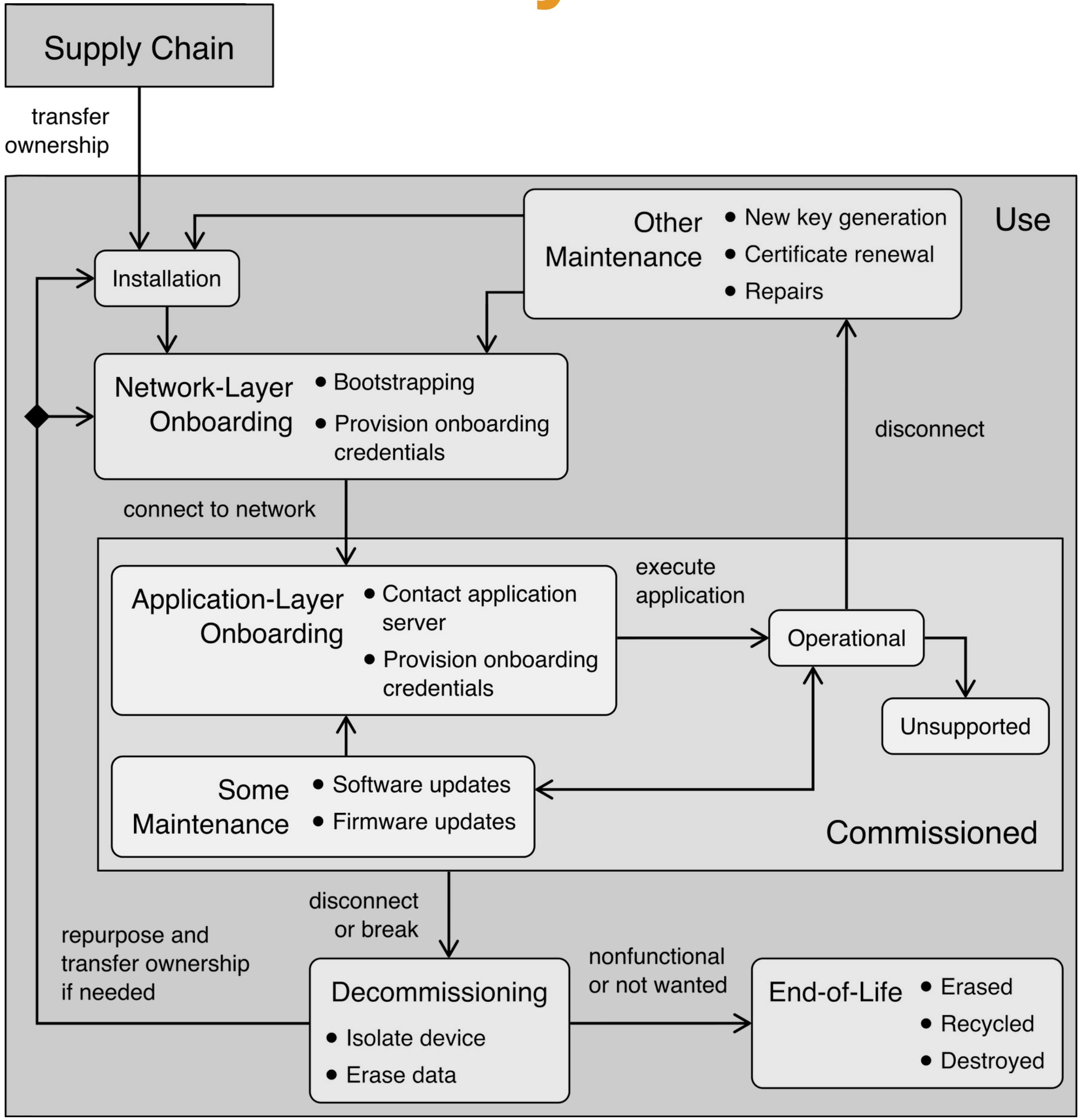
- Manufacturers perform tasks to make the device onboarding-ready

- Various integrators may have to connect the device to their own networks as part of the manufacturing process


Supply Chain
Research, Design, and Development
Manufacturing
Production
● Install onboarding-related chipset
● Install bootstrapping credentials, including identity imprint and keys
● Establish manufacturer as owner
● Pass control to various integrators
transfer ownership or authorize to onboard
return ownership or control
Integration
● Installation
● Network-layer onboarding
● Connect to network
● Perform integration
● Disconnect
production complete
Homologation
Rebranding
Transport
Storage
Shelf Life
transfer ownership
Use

Onboarding-Related Aspects of Lifecycle Management (Use Phase)

- Devices may have to be re-onboarded repeatedly during their lifetime due to
  - Refresh credentials periodically
  - Network security breach
  - Device maintenance
  - Device repurposing
  - Device resale



Onboarding Security Characteristics and Capabilities*

*(not the complete list)

Characteristic	Definition
Device Identity	Device should have a unique identifier that's privacy-preserving
Device Authent.	The network can verify the device's asserted identity
Network Selection	The network's identifier can be provisioned to the device
Network Authent.	The device can verify the network's asserted identity
Secure Local Credentialing	Locally-significant, device-specific credentials can be provisioned automatically, over a secure channel; late binding of credentials
Encryption details	Crypto is configurable; public/private key pair support
Privacy	Info added after manufacture can be deleted by authorized user
Device Intent	Information (e.g., MUD URL) is conveyed over a secure channel
Trusted Onboarder	Must the person performing the onboarding be trusted or not?
Device Attestation	Onboard only after verification of some device elements
Proof of ownership	Supports verification that a device has a specific owner

Enterprise vs. Home Use*

Characteristic	Home Use Case	Enterprise Use Case
Ease of use	Required	Desirable, but not required
Network technology	WiFi	Wired and WiFi
Ease of Integration	Required	Some effort is tolerable
Bulk onboarding	Manual operation ok	Hands-free operation required
Proof of Ownership	Probably not required	Desirable for strong security
Internet Access req'd?	Not required	Desirable; probably required
App-layer onboarding	Desirable	Desirable; probably required
Device accessible?	Yes	May be difficult to reach
Regulatory compliance	Not typically a concern	Mandatory for some sectors

* not the complete list

Observations on t2trg-secure-bootstrapping

The t2trg document surveys current options for what we define as network-layer onboarding

The t2trg recommendations for use of the terms "bootstrapping" and "provisioning/configuring" are reasonably consistent with our onboarding steps "bootstrapping" and "provisioning"

Document goals are different

- As a survey, t2trg is agnostic with respect to specific requirements for secure bootstrapping.
- NCCoE white paper defines minimum requirements for trusted onboarding

NCCoE whitepaper establishes a generic model with well-defined roles and a robust list of characteristics for the onboarding lifecycle

NCCoE IoT Onboarding Project

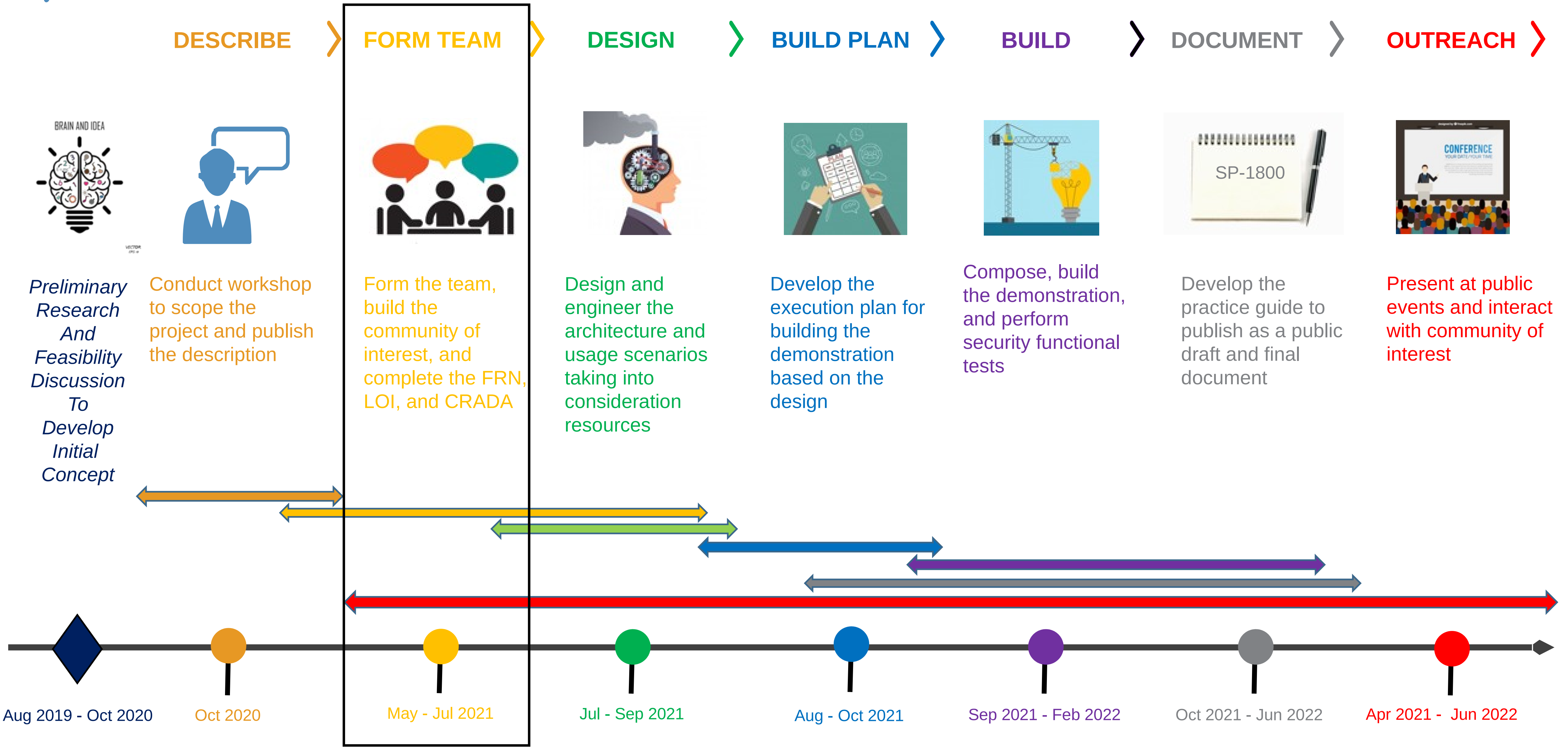
Trusted IoT Device Onboarding and Lifecycle Management:
Enhancing IP-Based IoT Device and Network Security

- Network-layer onboarding
- Integrate additional capabilities to secure the full device lifecycle
  - e.g., application-layer onboarding, MUD, attestation, lifecycle management

Opportunity for cross-pollination

- Knowledge developed and learned form the project can help guide standards

Estimated Project Execution Timeline



Preliminary Research And Feasibility Discussion To Develop Initial Concept

Aug 2019 - Oct 2020

DESCRIBE

Conduct workshop to scope the project and publish the description

Oct 2020

FORM TEAM

Form the team, build the community of interest, and complete the FRN, LOI, and CRADA

May - Jul 2021

DESIGN

Design and engineer the architecture and usage scenarios taking into consideration resources

Jul - Sep 2021

BUILD PLAN

Develop the execution plan for building the demonstration based on the design

Aug - Oct 2021

BUILD

Compose, build the demonstration, and perform security functional tests

Sep 2021 - Feb 2022

DOCUMENT

Develop the practice guide to publish as a public draft and final document

Oct 2021 - Jun 2022

OUTREACH

Present at public events and interact with community of interest

Apr 2021 - Jun 2022

Thank You!

Questions?

Please send follow-up email to:
iot-onboarding@nist.gov

References

NIST Cybersecurity White Paper:

- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.09082020-draft.pdf

NCCoE Virtual Workshop:

- https://www.nccoe.nist.gov/events/virtual-workshop-trusted-iot-device-network-layer-onboarding-and-lifecycle-management

NCCoE Project Page with Project Description:

- https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding

Backup Slides

What is Trusted Network Layer Onboarding?

Network-Layer Onboarding

- Steps needed to provision a device with its network credentials
  - Performed when the device is deployed (not when it is manufactured)

Trusted Network-layer Onboarding

- Device is provisioned with unique credentials
- Device and network have the opportunity to authenticate each other
- Provisioning occurs over an encrypted channel
- No humans are given access to the credentials
- Can be performed throughout the device lifecycle

Trusted Onboarding Basics

Network Onboarding Component

A logical component that acts on behalf of the network to onboard devices using the *network onboarding protocol*

Network bootstrapping credentials

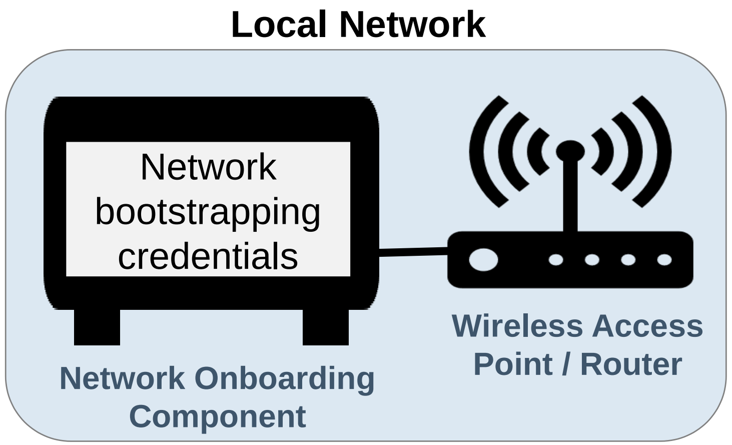
Credentials the network needs so it can be authenticated by the device (e.g., unique ID and private key)

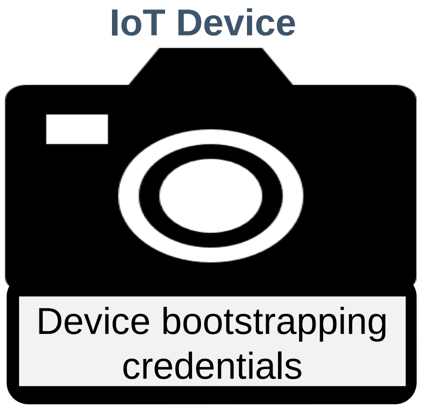
Device bootstrapping credentials

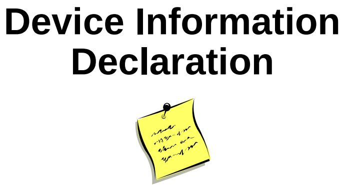
Credentials the device needs to establish communications with and be authenticated by the network onboarding component. Provisioned when the device is manufactured (e.g., unique ID, private key, Wi-Fi channel). May also include additional information such as MUD URL and application-layer bootstrapping credentials)

Device Information Declaration (optional)

Signed digital assertion of info about the device, such as its owner and any entities authorized to onboard the device

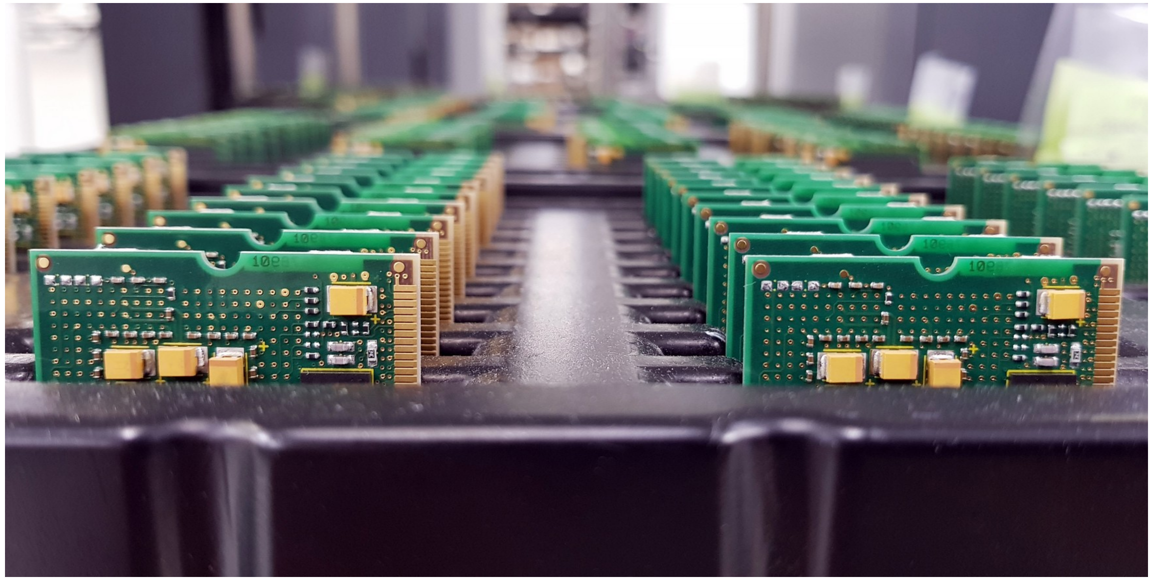

Local Network
Network bootstrapping credentials
Network Onboarding Component
Wireless Access Point / Router





Onboarding Characteristics of Interest to Manufacturers and Vendors*

- Specification Status
- Is it proprietary?
- Owning Body
- Implementation Status/Maturity
- Who Implements It?
- Manufacturing Complexity
- Regulatory Compliance
- Certification Program
- IoT Device Requirements
- Proof of ownership



- Type of secure storage required
- Memory, power, size, wired/wireless
- Bootstrapping information inserted by manufacturer (identity, private key, device intent info, application-layer bootstrapping info)

* not the complete list