Welcome to the National Cybersecurity Center of Excellence

Trusted IoT Onboarding: An Introduction to NIST SP 1800-36

Wednesday, November 1st, 2023 | 10:00 – 11:30 AM (EDT)

We will begin shortly.
This webinar will be recorded.

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

Agenda

Time (ET)	Session	Speaker(s)
10:00–10:05 a.m.	Welcome and Introduction	• Cherilyn Pascoe, Director, NIST NCCoE • Paul Watrobski, Principal Investigator, NIST NCCoE
10:05–10:15 a.m.	Project Overview • Cybersecurity problem, general build architecture, and publication status of NIST SP 1800-36	• Paul Watrobski, Principal Investigator, NIST NCCoE
10:15–10:20 a.m.	Volume E • Cybersecurity Mapping	• Susan Symington, Cyber Architecture and Resiliency Principal, NCCoE/MITRE
10:20–10:30 a.m.	Build 1 • Discussion on Trusted Network-Layer Onboarding with Wi-Fi Easy Connect	• Dan Harkins, Fellow, HPE Aruba • Danny Jump, Senior Product Manager, HPE Aruba
10:30–10:40 a.m.	Build 2 • Discussion on Trusted Network-Layer Onboarding with Wi-Fi Easy Connect	• Craig Pratt, Lead Software Engineer, CableLabs • Darshak Thakore, Principal Architect, CableLabs • Andy Dolan, Senior Security Engineer, CableLabs
10:40–10:50 a.m.	Build 3 • Discussion on Trusted Network-Layer Onboarding with BRSKI	• Michael Richardson, Chief Scientist, Sandelman Software Works

Agenda cont.

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Time (ET)	Session	Speaker(s)
10:50–10:58 a.m.	Build 4 • Discussion on Trusted Network-Layer Onboarding with the Thread Protocol	• Brecht Wyseur, Senior Product Manager and Product Strategy, Kudelski IoT
10:58–11:06 a.m.	Build 5 • Discussion on Trusted Network-Layer Onboarding with BRSKI over Wi-Fi	• Nick Allott, CEO, NquiringMinds
11:06–11:14 a.m.	Factory Provisioning Use-Case (cross-build application) • Discussion on Factory Provisioning	• Steve Clark, Security Technologist, SEALSQ, a subsidiary of WISeKey • Michael Richardson, Chief Scientist, Sandelman Software Works
11:14–11:25 a.m.	Participant Q&A	All
11:25–11:30 a.m.	Closing Remarks • Review draft and next steps, join the COI, contact us	• Paul Watrobski, Principal Investigator, NIST NCCoE

Trusted IoT Onboarding: An Introduction to NIST SP 1800-36

Welcome

Cherilyn Pascoe, Director, NIST NCCoE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Trusted IoT Onboarding:
An Introduction to NIST SP 1800-36

Project Overview

Paul Watrobski, Principal Investigator, NIST NCCoE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SP 1800-36 Practice Guide

NIST SPECIAL PUBLICATION 1800-36A

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

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume A:
Executive Summary

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

Blaine Mulugeta
Susan Symington
The MITRE Corporation
McLean, Virginia

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

William Barker
Dakota Consulting
Silver Spring, Maryland

Michael Richardson
Sandelman Software Works
Ottawa, Ontario

December 2022

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

Volume A
Executive Summary

NIST SPECIAL PUBLICATION 1800-36B

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

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume B:
Approach, Architecture, and Security Characteristics

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

William Barker
Dakota Consulting
Silver Spring, Maryland

Chelsea Deane
Joshua Klosterman
Charlie Rearick
Blaine Mulugeta
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

Peter Romness
Cisco
San Jose, California

Tyler Baker
David Griego
Foundries.io
London, United Kingdom

Brecht Wyseur
Kudelski IoT
Cheseaux-sur-Lausanne, Switzerland

Alexandru Mereacre
Nick Allott
NquiringMinds
South Hampton, United Kingdom

Julien Delaplanke
NXP Semiconductors
Mougins, France

Michael Richardson
Sandelman Software Works
Ontario, Canada

Mike Dow
Steve Egerter
Silicon Labs
Austin, Texas

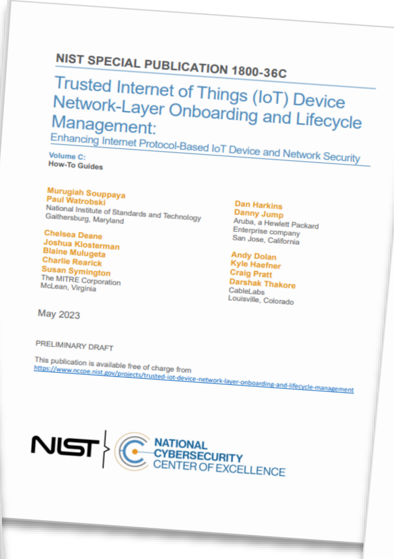
Steve Clark
WISeKey
Geneva, Switzerland

May 2023

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

Volume B
Approach & Architecture



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

May 2023

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

Volume C
How-To Guide

NIST SPECIAL PUBLICATION 1800-36D

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

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume D:
Functional Demonstrations

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

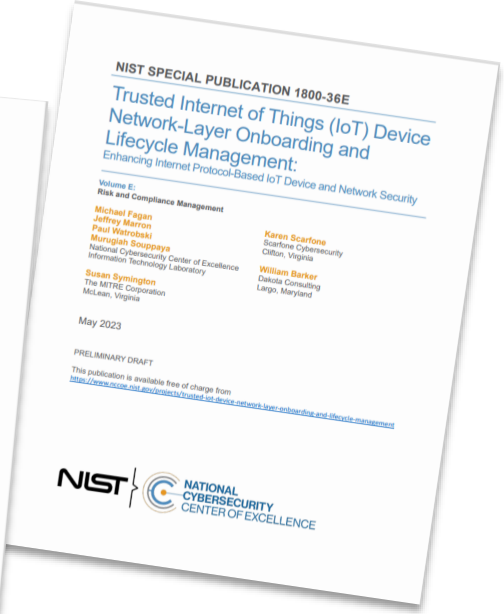
Chelsea Deane
Joshua Klosterman
Charlie Rearick
Blaine Mulugeta
Susan Symington
The MITRE Corporation
McLean, Virginia

May 2023

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

Volume D
Functional Demonstrations



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

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

William Barker
Dakota Consulting
Largo, Maryland

May 2023

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

Volume E
Risk & Compliance Management

Preliminary Drafts

Trusted IoT Network-Layer Onboarding: Objective

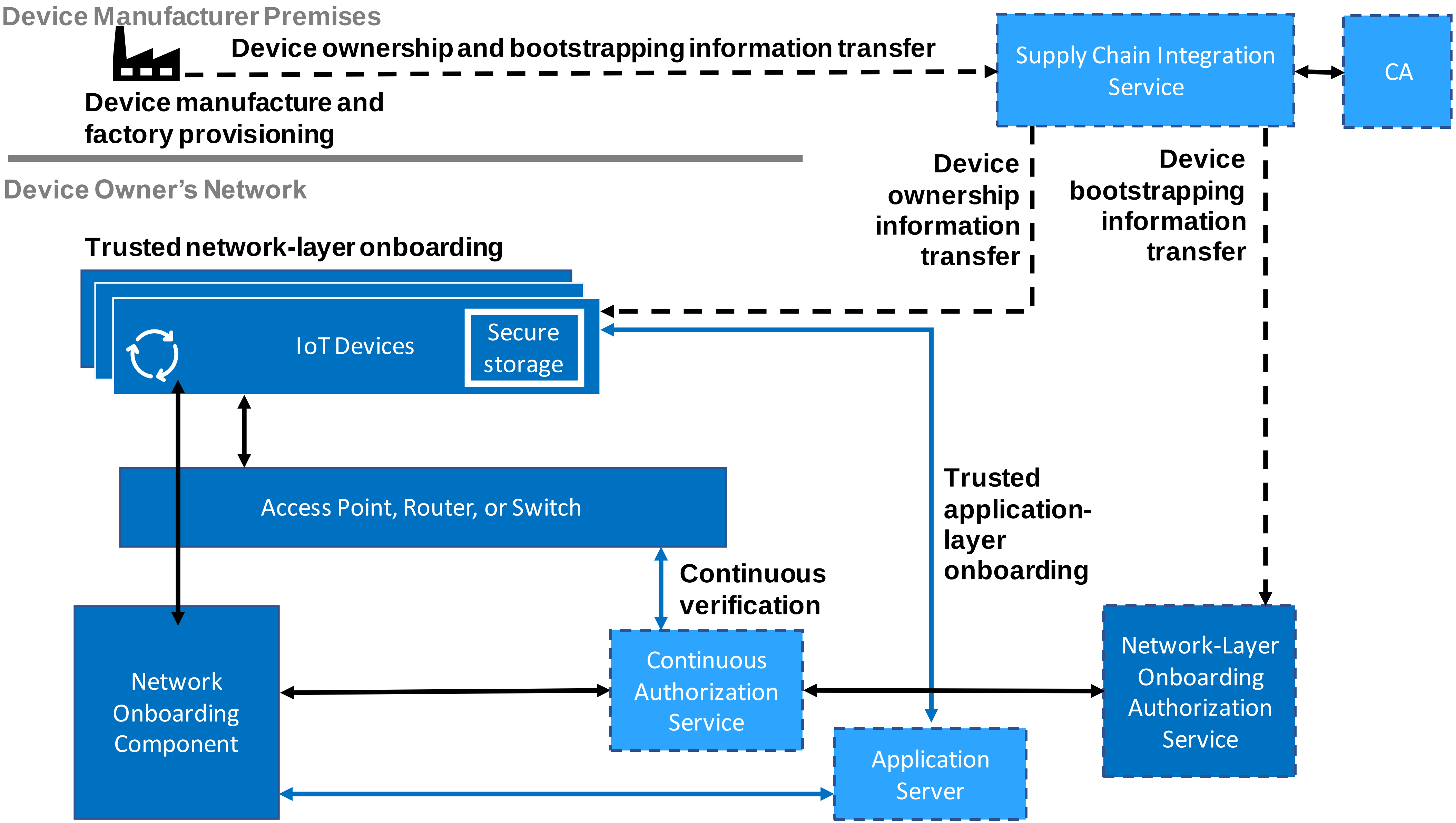
- Number of IoT devices is rapidly growing
  - Estimated 40 billion IoT devices by 2025
  - The growing number of IoT devices is leading to an expanding attack surface
  - We need scalable mechanisms to safely manage IoT devices throughout their lifecycles
    - ➢ Network credential provisioning
    - ➢ Device intent (e.g. MUD – Manufacturer Usage Description)
    - ➢ Device attestation
    - ➢ Application-layer onboarding
    - ➢ Additional zero-trust-inspired mechanisms

Sources: Statista: • Number of connected devices worldwide 2030 | Statista (38.6 billion)
International Data Corporation (IDC): 41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025 - Help Net Security (41.6 billion)

Trusted IoT Network-Layer Onboarding: Scope

- *Network Layer Onboarding:*
  - Provisioning of network credentials to a device
  - Performed when the device is deployed (not when it is manufactured)
- ***Trusted*** *Network-Layer Onboarding* - provides assurance that a network is not put at risk as new IoT devices are added to it
  - 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 repeatedly throughout the device lifecycle

High Level Architecture



Device Manufacturer Premises

Device ownership and bootstrapping information transfer

Device manufacture and factory provisioning

Device Owner’s Network

Trusted network-layer onboarding

Supply Chain Integration Service
CA
Device ownership information transfer
Device bootstrapping information transfer
IoT Devices
Secure storage
Access Point, Router, or Switch
Trusted application-layer onboarding
Continuous verification
Network Onboarding Component
Continuous Authorization Service
Application Server
Network-Layer Onboarding Authorization Service

Current Scenarios

- **Scenario 0: Factory Provisioning**
  - This scenario, which simulates the IoT device factory provisioning process, is designed to represent some high-level steps that must be performed in the factory before the device is transferred to its first post-production owner (e.g., device birth credentials, bootstrapping information, etc.).
- **Scenario 1: Trusted Network-Layer Onboarding**
  - Identities of the device and the network are authenticated.
  - Network onboarding component provisions unique network credentials to the device over a secure channel.
- **Scenario 2: Trusted Application-Layer Onboarding**
  - Trusted application-layer onboarding that is performed automatically on an IoT device after it connects to a network.
- **Scenario 3: Re-Onboarding a Wiped Device**
  - Re-onboarding an IoT device to a network after wiping it clean of any stored data so that it can be re-credentialed and re-used.
- **Scenario 4: Ongoing Device Validation**
  - Performing attestation, supply chain management (e.g., hardware, firmware, and software component inventory), configuration monitoring, or other asset-management-related operations on an IoT device to validate its authenticity and integrity.
  - May be performed as part of a trusted boot process or at some other point before permitting the device to be onboarded to the network.
- **Scenario 5: Establishing and Maintaining Credential and Device Security Posture Throughout the Lifecycle**
  - Downloading device firmware updates/patches.
  - Securely integrate a device intent enforcement mechanism (e.g., Manufacturer Usage Description [MUD]).
  - Establish and maintain the device's network credentials by provisioning X.509 certificates and updating expired credentials.

Builds

Current Builds

- Build 1: Wi-Fi Easy Connect Protocol, Aruba/HPE

  + Independent Application-Layer Onboarding to UXI Cloud
  - Collaborators: Aruba, an HPE Company (Build Champion), CableLabs, NXP Semiconductors, SEALSQ, a subsidiary of WISeKey
- Build 2: Wi-Fi Easy Connect Protocol, CableLabs, OCF

  + Streamlined Application-Layer Onboarding to OCF IoTivity
  - Collaborators: CableLabs (Build Champion), OCF, Aruba, an HPE Company, NXP Semiconductors, SEALSQ, a subsidiary of WISeKey
- Build 3: Bootstrapping Remote Key Infrastructure (BRSKI) Protocol, Sandelman Software Works
  - Collaborators: Sandelman Software Works (Build Champion), NXP Semiconductors, SEALSQ, a subsidiary of WISeKey, NquiringMinds
- Build 4: Thread Protocol, Silicon Labs, Kudelski IoT

  + Independent Application-Layer onboarding to AWS IoT Core
  - Collaborators: Kudelski IoT, Silicon Labs
- Build 5: Bootstrapping Remote Key Infrastructure (BRSKI) Protocol, NquiringMinds
  - Collaborators: NquiringMinds (Build Champion), Sandelman Software Works, SEALSQ, a subsidiary of WISeKey
- Factory Provisioning Use-Case (cross-build application)
  - Collaborators: Aruba, an HPE Company, Sandelman Software Works, SEALSQ, a subsidiary of WISeKey

Collaborators

CableLabs

cisco

FOUNDRIES.IO

Hewlett Packard Enterprise

KUDELSKI IOTHINGS

NXP

nquiringminds

OPEN CONNECTIVITY FOUNDATION®

SANDELMAN SOFTWARE WORKS

SEAL SQ semiconductors + quantum

SILICON LABS

Volume E: Risk and Compliance Management (NIST SP 1800-36E)

Maps between onboarding architecture functions and two cybersecurity documents:

NIST SP800-53r5
Security and Privacy Controls for Information Systems and Organizations

Framework for Improving Critical Infrastructure Cybersecurity (CSF) **subcategories**

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Susan Symington

Why Map?

- Mappings help organizations understand:
  - How trusted onboarding can help them achieve their cybersecurity goals
  - How trusted onboarding can be supported by their existing implementations
  - How to identify potential technology gaps

Our Mapping Objectives

- Identify why organizations should implement trusted network-layer onboarding and lifecycle management
  - Show how trusted onboarding can help fulfill security requirements
    - How trusted onboarding ***supports*** CSF subcategories and SP 800-53 controls

- Identify how organizations can implement trusted network-layer onboarding and lifecycle management
  - Show how trusted onboarding ***is supported by*** existing implementations of CSF subcategories and SP 800-53 controls

Example: Reference Architecture-to-CSF

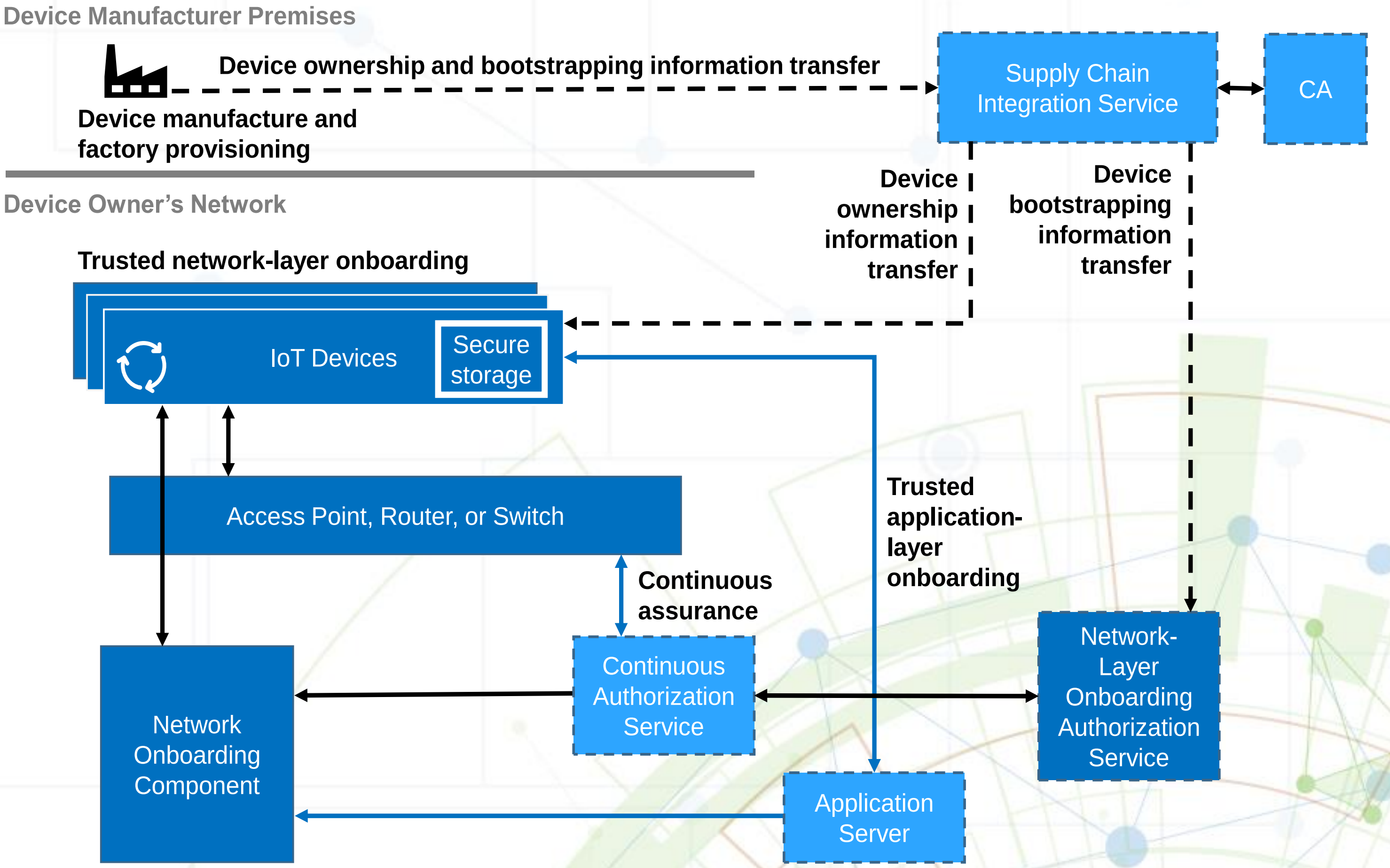
Onboarding Component	Component Cybersecurity Function	Relationship to CSF Subcategories	Relationship Explanation
Network-Layer Onboarding Component	Interacts with the IoT device using the onboarding protocol to securely provide local network credentials to the device. May also securely convey to the IoT device application-layer bootstrapping information, the identifier of the network to which the device should onboard, and device intent information.	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.
		Is Supported by (precedes) ID.AM-1: Physical devices and systems within the organization are inventoried	Device ownership information must be recorded and available in order to be able to determine whether the network is authorized to onboard the device.

Mapping Status

We mapped to functionality of:

- ➢ General reference architecture
- ➢ Specific onboarding protocols
  - ○ Wi-Fi Easy Connect
  - ○ BRSKI
- ➢ Specific project builds
  - ○ Build 1
  - ○ Other builds are in progress

We mapped to both CSF subcategories and SP 800-53 controls in each case



Device Manufacturer Premises
Device ownership and bootstrapping information transfer
Device manufacture and factory provisioning
Supply Chain Integration Service
CA
Device Owner's Network
Device ownership information transfer
Device bootstrapping information transfer
Trusted network-layer onboarding
IoT Devices
Secure storage
Access Point, Router, or Switch
Continuous assurance
Trusted application-layer onboarding
Network Onboarding Component
Continuous Authorization Service
Network-Layer Onboarding Authorization Service
Application Server

Mapping Elements

Build 1: Wi-Fi Easy Connect Protocol, Aruba/HPE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Dan Harkins

Danny Jump

aruba

a Hewlett Packard Enterprise company

Device Provisioning Protocol– DPP

Robust and secure on-boarding per NIST CSWP on Network-Layer Onboarding and Lifecycle Management

Phases of DPP map closely with description of process in NIST CSWP

- Bootstrapping– establishment of trust in a thing's public key
    - DPP URI contains base64-encoded public key of thing
    - Cloud-based, QR code based, NFC-based bootstrapping; also a Password Authenticated Key Exchange can be used to parlay a simple passcode into a trusted public keys
- Authentication– strong authentication of device by network, weaker authentication of network by device
- Provisioning– configuring network credentials in device
- Network Access– secure connection to network to enable application-layer onboarding

Uses 802.11 action frames (pre-association, no SSID, no soft-AP) a Hewlett Packard Enterprise company

Onboarding for Enterprise

Transfer of ownership of *thing*

- Purchase order transfers DPP URI from vendor cloud using open published REST API framework
- Network onboarding equipment acquires DPP URIs for all purchased *things*
- No soft-AP so no rogue APs, no extra SSIDs beaconing, on enterprise network

DPP Presence Announcement issued by unprovisioned *things*

- 802.11 action frame consisting of a hash of “chirp” + bootstrapping key
- Network onboarding equipment is able to identify things by chirps
- Only equipment that possesses a thing’s DPP URI is able to provision *thing*

Trust by *thing*

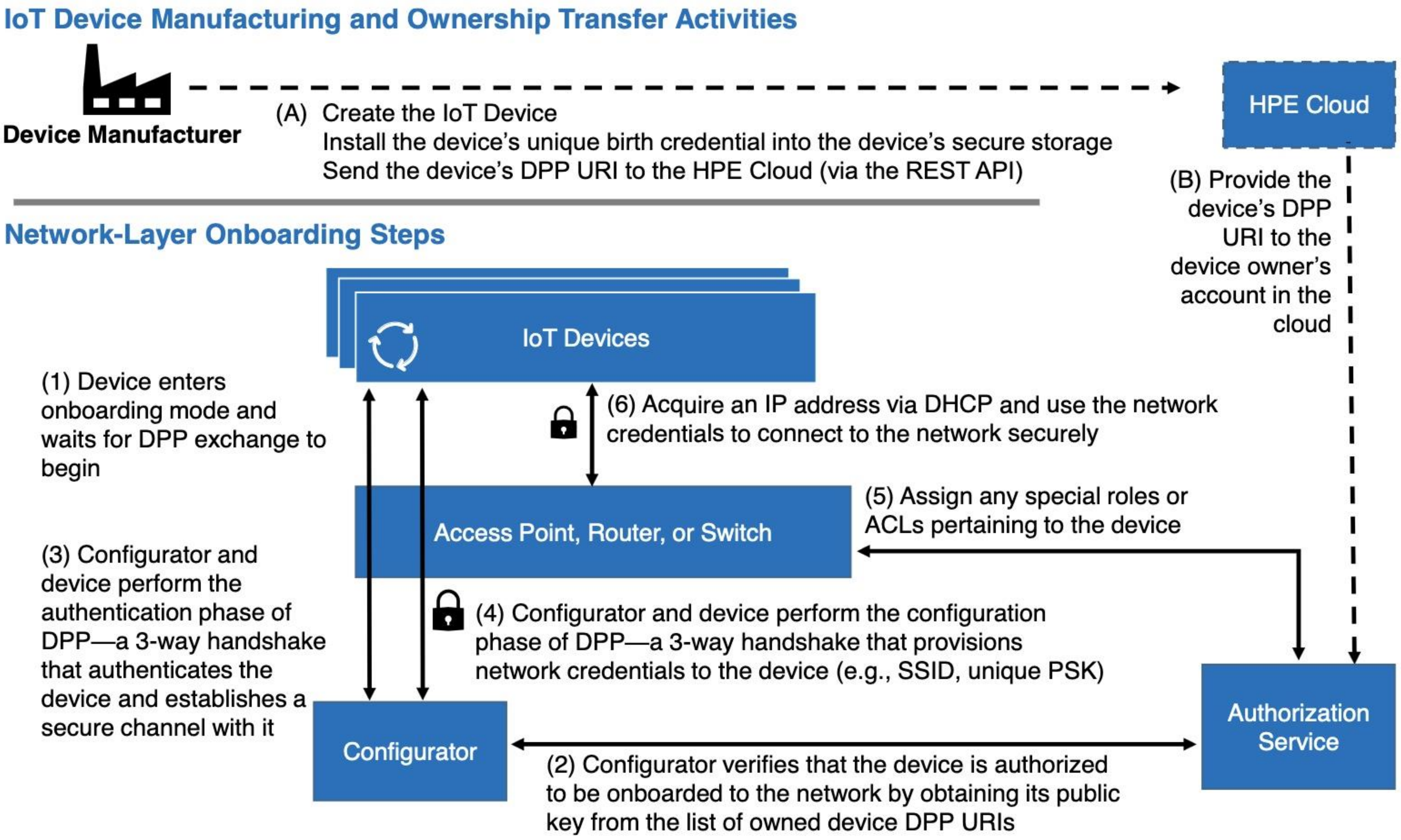
- Manufacturer/vendor trusted to not gratuitously expose bootstrapping key
- The only entity that knows its public bootstrapping key is its legitimate owner

Trust by Network

- Vendor/manufacturer is trusted to provide correct DPP URIs for *things*
- *Thing* proves possession of corresponding private key

aruba
a Hewlett Packard Enterprise company

Build 1 and the Notional Architecture



IoT Device Manufacturing and Ownership Transfer Activities

Device Manufacturer

(A) Create the IoT Device
Install the device's unique birth credential into the device's secure storage
Send the device's DPP URI to the HPE Cloud (via the REST API)

HPE Cloud

(B) Provide the device's DPP URI to the device owner's account in the cloud

Network-Layer Onboarding Steps

IoT Devices

(1) Device enters onboarding mode and waits for DPP exchange to begin

(6) Acquire an IP address via DHCP and use the network credentials to connect to the network securely

Access Point, Router, or Switch

(5) Assign any special roles or ACLs pertaining to the device

(3) Configurator and device perform the authentication phase of DPP—a 3-way handshake that authenticates the device and establishes a secure channel with it

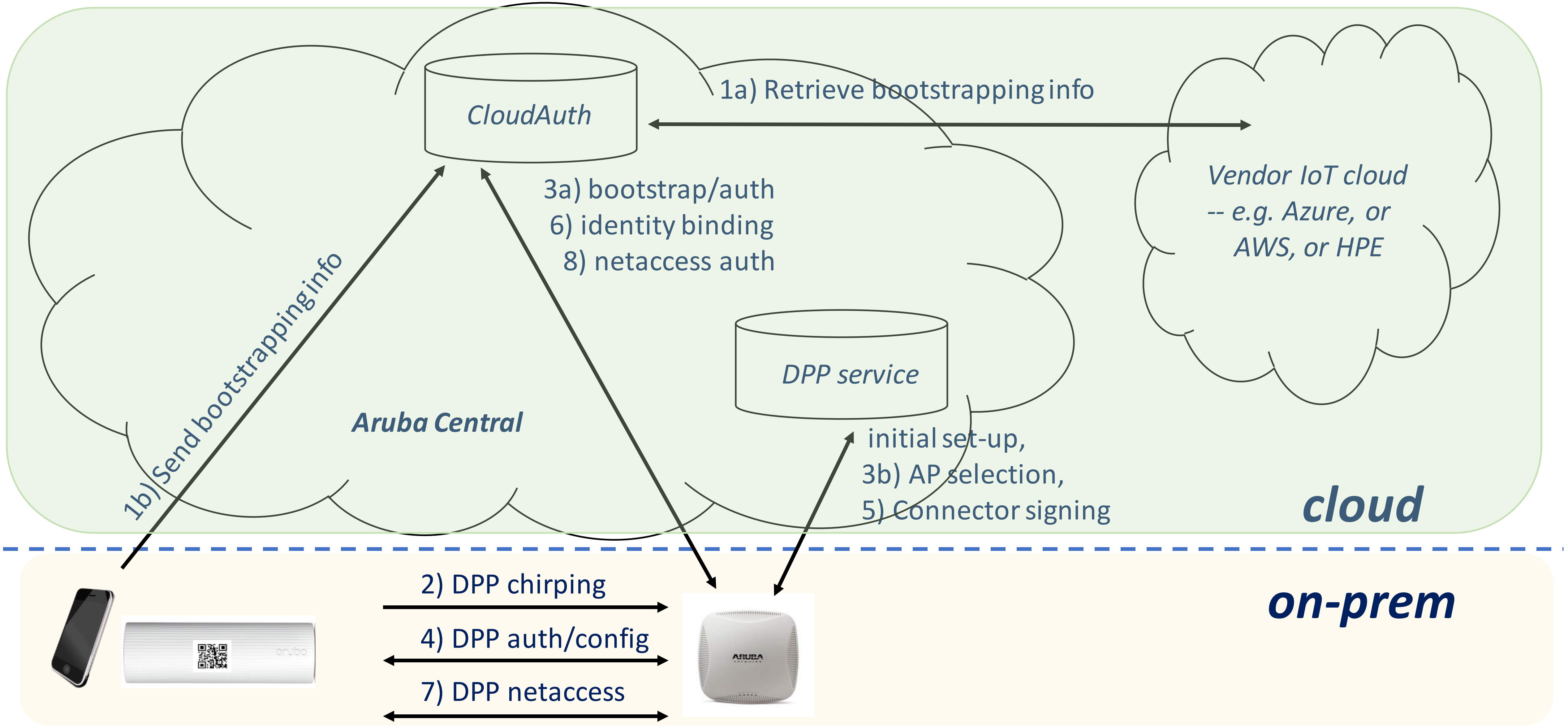
(4) Configurator and device perform the configuration phase of DPP—a 3-way handshake that provisions network credentials to the device (e.g., SSID, unique PSK)

Configurator

Authorization Service

(2) Configurator verifies that the device is authorized to be onboarded to the network by obtaining its public key from the list of owned device DPP URIs

Build 1's DPP Architecture– DPP As A Service



Network Layer Credentials with DPP

DPP Provisioning provides SSID and credential to access network to *thing*

Wide support for credentials used in 802.11 today

- Pre-shared key for WPA2-PSK AKM
- Password for WPA3-SAE AKM
- X.509 certificate for WPA3-Enterprise (including WPA3-CNSA) AKM
  - RSA and ECC support
  - RFC 7030-style CSR Attributes request
  - PKCS10/PKCS7 exchange with client proof-of-possession (of private key)
- Connector– a signed ECC public key for DPP AKM

Network access with DPP Connector

- Client and AP exchange connectors signed by same authority
- Client and AP do Diffie-Hellman using public key from peer’s connector
- Resulting secret becomes PMK, then 4-way handshake, etc

Build 1 Capabilities

Current

Trusted Network-Layer Onboarding

- Device authentication and authorization by network
- Network authorization by device
- Provisioning of a network profile for secure access
- Provisioning of a unique device-specific credential
- Network segmentation– assigning *thing* to a network segment

Application-Layer Onboarding

Device Re-Onboarding

Planned

Integration with public, trusted CA for certificate issuance

MUD

Benefits of DPP

DPP workflow is, “plug it in, turn it on…you’re done”

Misuse resistance: easy to use correctly, difficult to use incorrectly

- QR codes scan or they don’t, once scanned there is nothing else to do
- Manufacturers and vendors have transfer of ownership of things worked out

No IoT or networking expertise needed to onboard things

- Industrial deployment (e.g. nuclear power plant, or off-shore oil rig) allow for *things* to be installed by a crew with no IT skills– just mount the device, apply power
- Homeowner just unpacks, scans, plugs device in
- Chirping device will be discovered and provisioned automatically

Simple, secure, robust onboarding workflow

No rigid onboarding process to follow– bootstrapping can take place before or after device is installed

Onboarding at scale and zero touch onboarding

CableLabs®

Security and Privacy Team

Build 2: Wi-Fi Easy Connect, CableLabs, OCF

Craig Pratt
Lead Software Architect
c.pratt@cablelabs.com

Darshak Thakore
Principal Architect
d.thakore@cablelabs.com

Andy Dolan
Senior Security Engineer
a.dolan@cablelabs.com

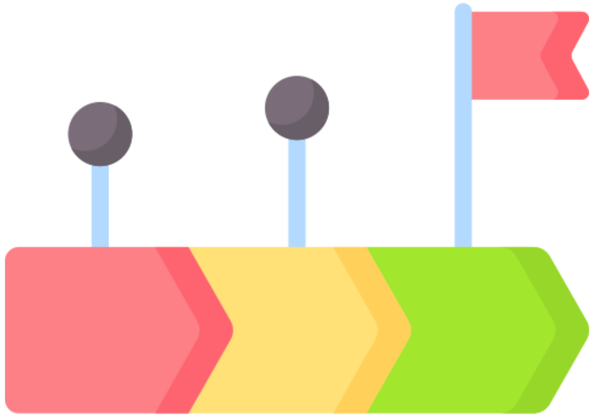
Network Onboarding with Custom Connectivity

a.k.a NetReach

Wi-Fi Network Onboarding: Goals

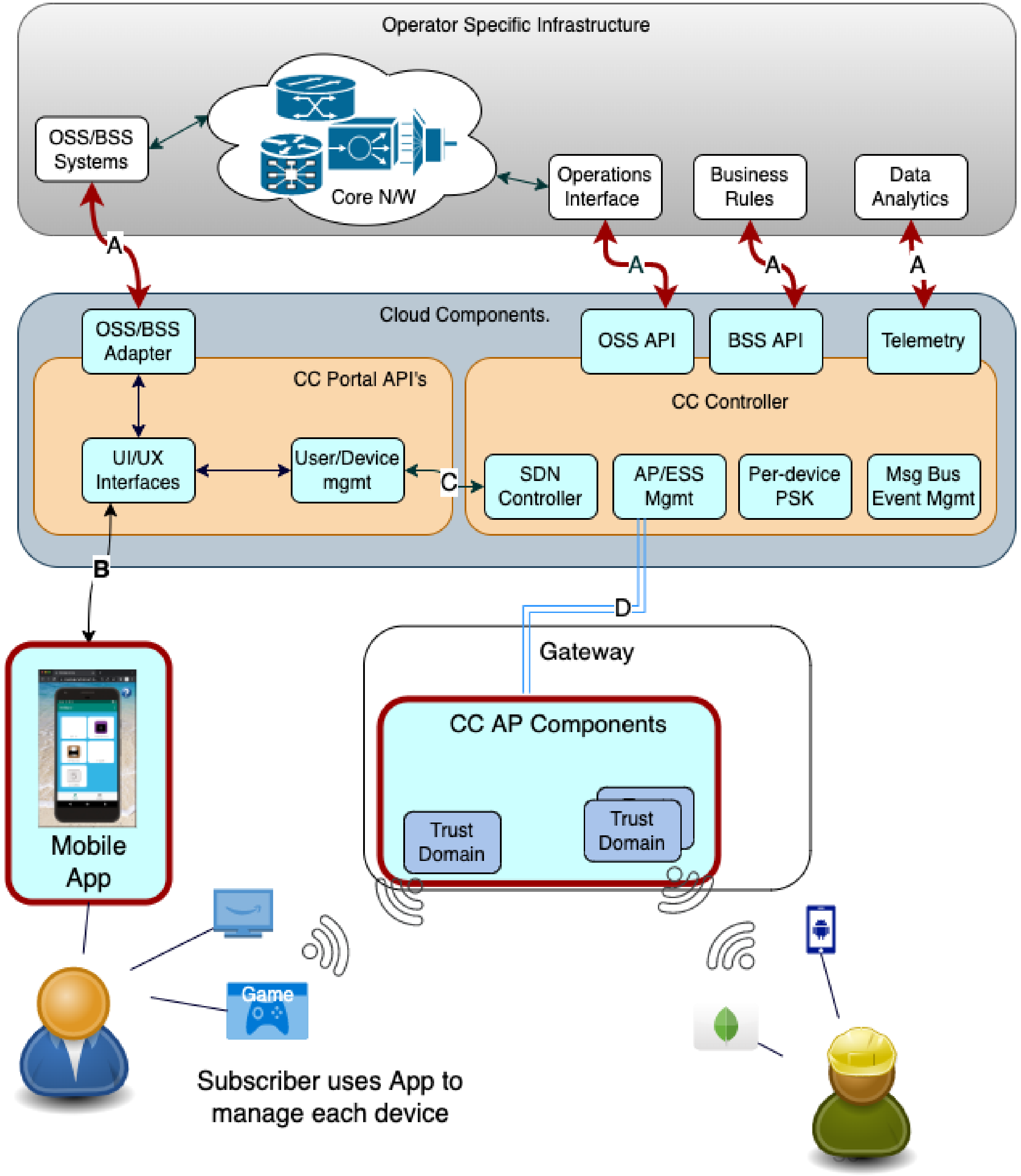
To demonstrate:

- Secure network (L2/L3) onboarding
  - Using DPP/EasyConnect and Custom Connectivity (NetReach) technology
- Provisioning of per-device credentials and policy for Wi-Fi devices
  - Including steering into network microsegments (Micronets)
- The secure conveyance of metadata during network onboarding
  - To facilitate application-layer (L4/L5) onboarding

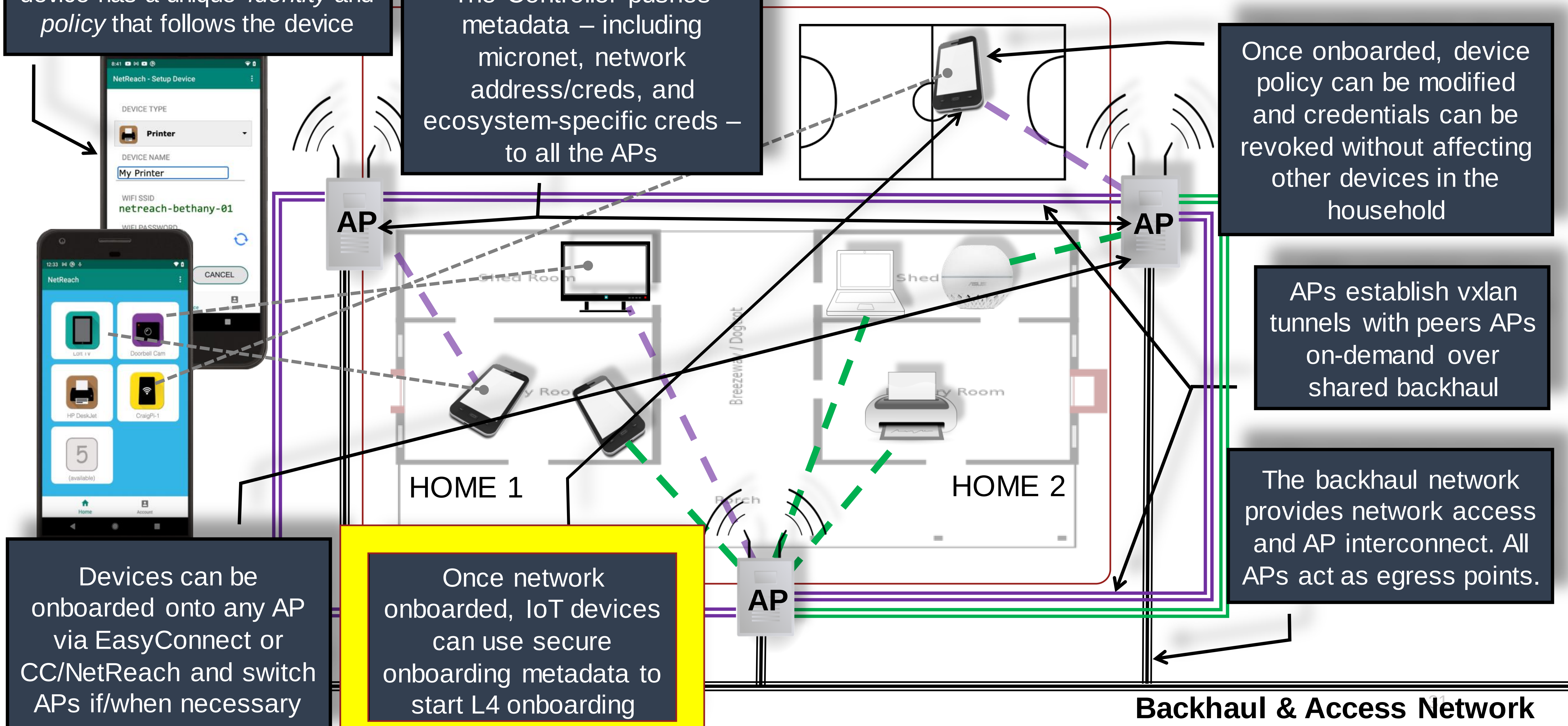


NetReach/CC Architecture

- **Network Onboarding Component**:
  - DPP/EasyConnect
  - CC/NetReach
- **Authorization Service**:
  - The CC (NetReach) Controller
- **AP/Router/Switch:**
  - AP agent controls inter-AP mesh, switch and router using SDN rules
- **Supply Chain Integration Service:**
  - Not provided
- **IoT Devices**
  - DPP-enabled Wi-Fi devices
  - Non-DPP Wi-Fi WPA2 devices



Subscriber uses App to manage each device



The CC/NetReach onboarding system enables devices to be given *unique* credentials. Each device has a unique *identity* and *policy* that follows the device

The Controller pushes metadata – including micronet, network address/creds, and ecosystem-specific creds – to all the APs

Once onboarded, device policy can be modified and credentials can be revoked without affecting other devices in the household

APs establish vxlan tunnels with peers APs on-demand over shared backhaul

The backhaul network provides network access and AP interconnect. All APs act as egress points.

Devices can be onboarded onto any AP via EasyConnect or CC/NetReach and switch APs if/when necessary

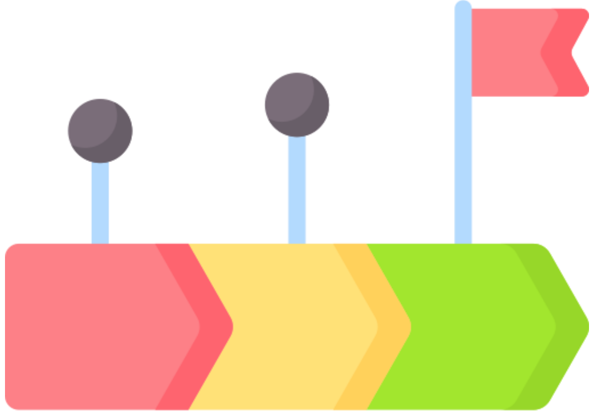
Once network onboarded, IoT devices can use secure onboarding metadata to start L4 onboarding

Streamlined Onboarding

(Application-layer onboarding)

Streamlined Onboarding: Goals

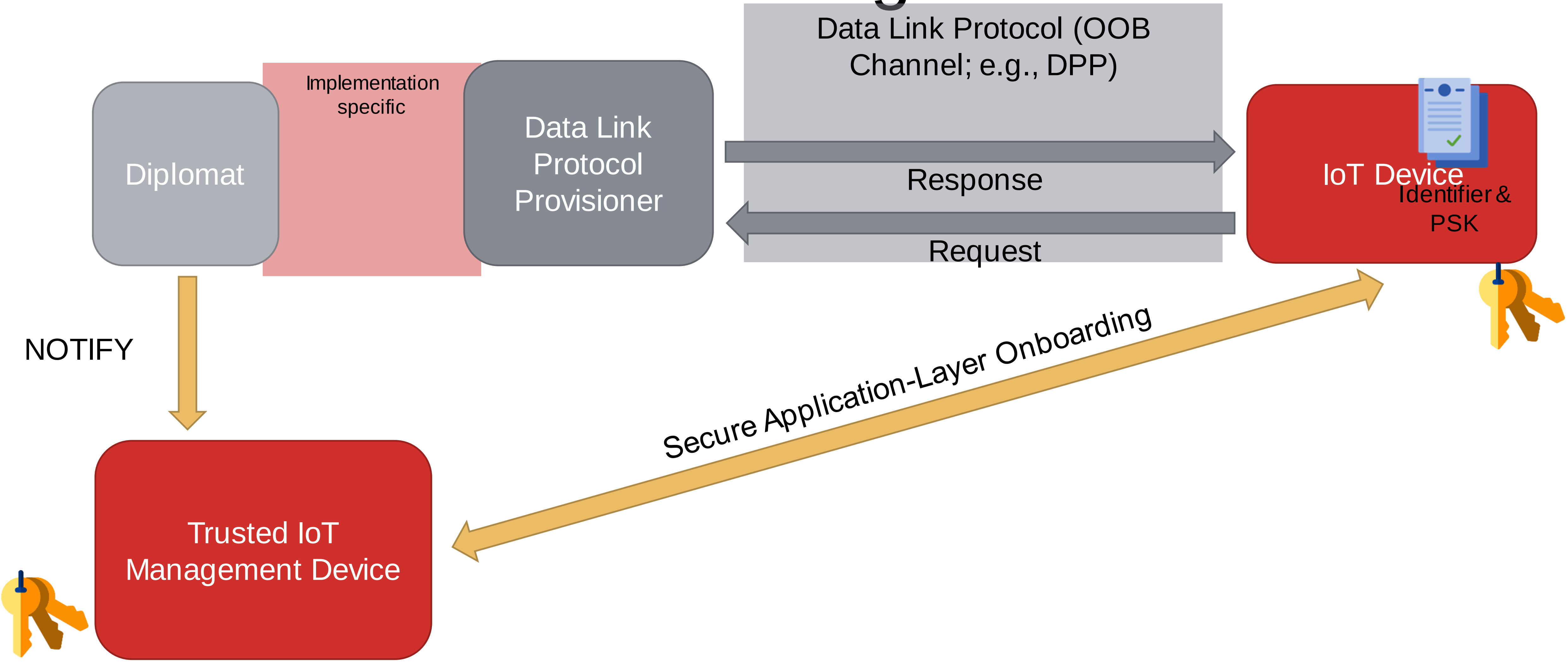
- Secure network onboarding establishes trust
  - Why not build upon that established trust at the application layer?
- Streamlined onboarding: Onboard application-layer framework using established trusted channel
  - *Any* application-layer framework
- Single administrative action to securely onboard device at all layers
- Simpler, and more secure



General Architecture and Flow

- A secure out of band (OOB) channel carries application-level information from the Device to the application-level management device (e.g., OCF)
  - Device identifier (e.g., initial UUID)
  - Authentication material (e.g., PSK, public key, certificate)
- Management device uses this information to:
  - Find device and initiate application-level onboarding
  - Authenticate device
- Mutual authentication possible with bidirectional OOB channel

Streamlined Onboarding Overview



Diagramat

Implementation specific

Data Link Protocol Provisioner

Data Link Protocol (OOB Channel; e.g., DPP)

Response

Request

IoT Device

Identifier & PSK

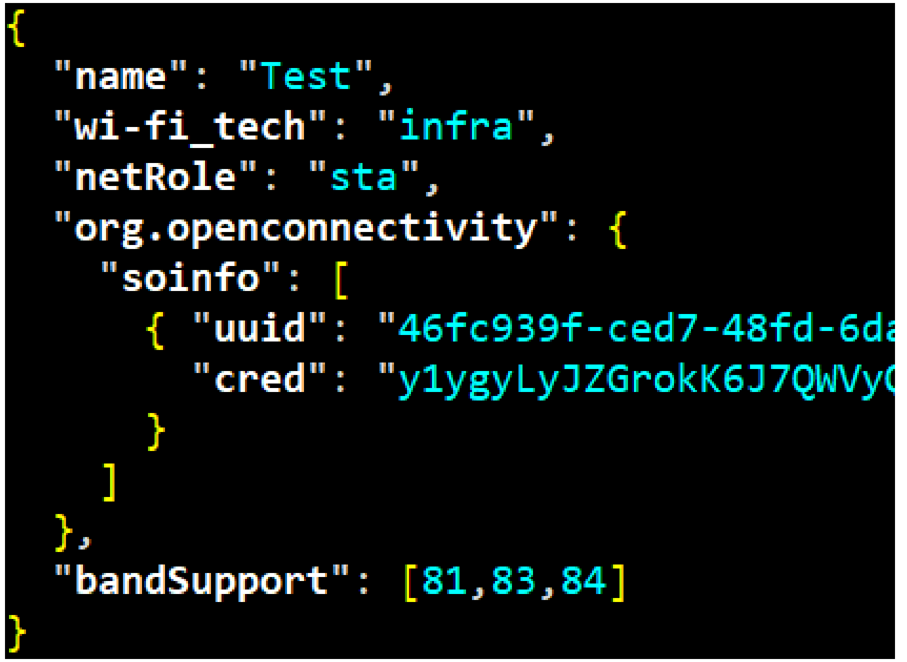
NOTIFY

Secure Application-Layer Onboarding

Trusted IoT Management Device

Streamlined Onboarding Implementation

- OCF implementation built with IoTivity-Lite
- Wi-Fi Easy Connect specification update for third-party information
- Modified `hostapd` and `wpa_supplicant`
  - Send streamlined onboarding information as part of DPP exchange
- DPP Diplomat runs alongside `hostapd`, forwards information to OBT



```
{
  "name": "Test",
  "wi-fi_tech": "infra",
  "netRole": "sta",
  "org.openconnectivity": {
    "soinfo": [
      { "uuid": "46fc939f-ced7-48fd-6da
        "cred": "y1ygyLyJZGrokK6J7QWVy
      }
    ]
  },
  "bandSupport": [81,83,84]
}
```

Example DPP configuration request message with Streamlined Onboarding info.

Craig Pratt
Lead Software Architect
c.pratt@cablelabs.com

Darshak Thakore
Principal Architect
d.thakore@cablelabs.com

Andy Dolan
Senior Security Engineer
a.dolan@cablelabs.com

NCCoE IoT Onboarding

Build 3: BRSKI - Operational Run Through

Michael Richardson,
Sandelman Software Works

June 2023 - Network Diagram for Build 3

Goals of iteration 1

- ~~Validation of~~
- ~~Registrar Validation~~
- ~~of MASA Verification~~
- ~~of IDevID~~

Testing with Secure Element (build 6)

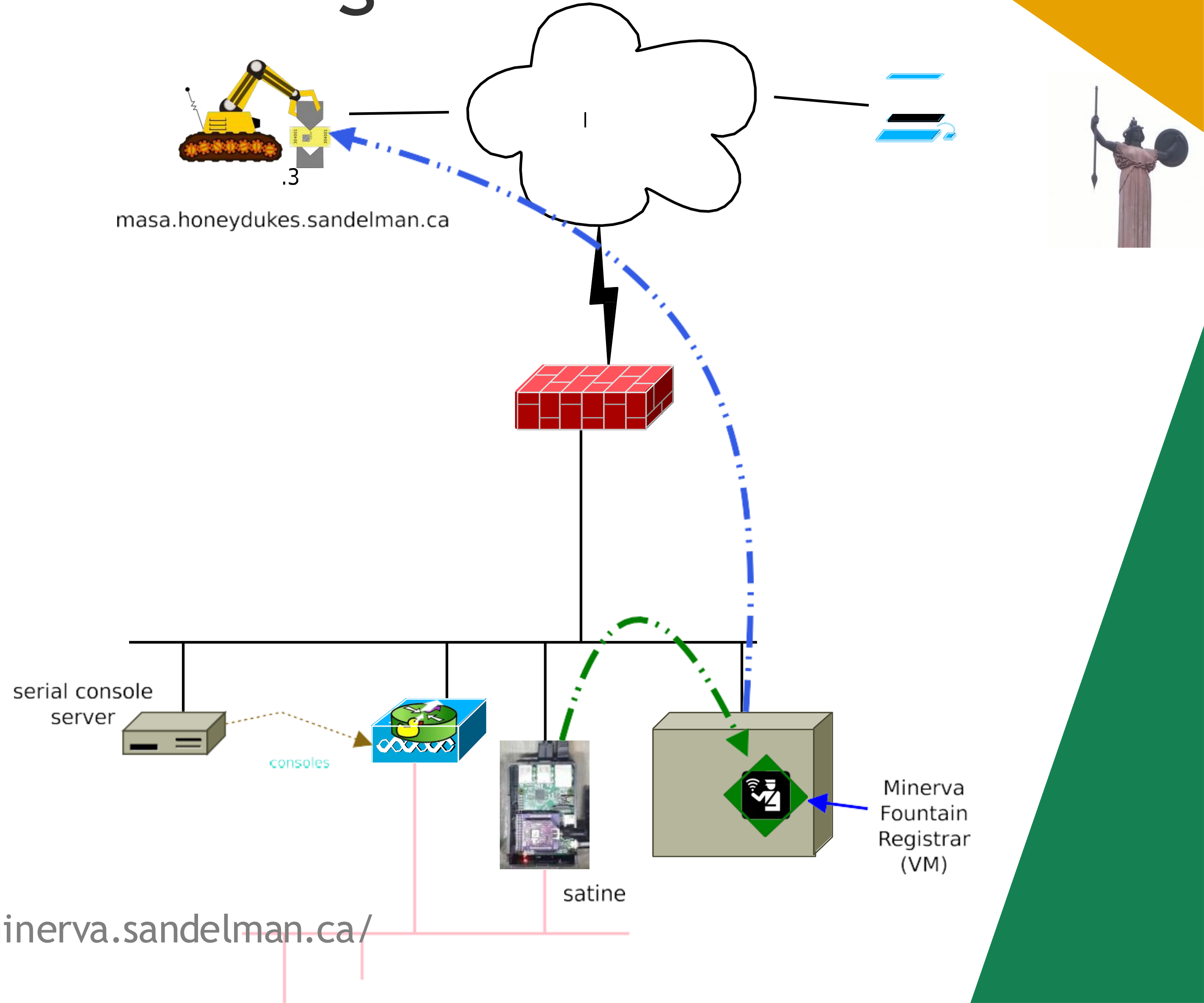
Testing with Build 5 vouchers/infrastructure

Goals of iteration 2

- Validation of Registrar/Join-Proxy
- Auto-discovery of Join-Proxy by Pledge

Goals of iteration 3

- Use of WIFI for onboarding

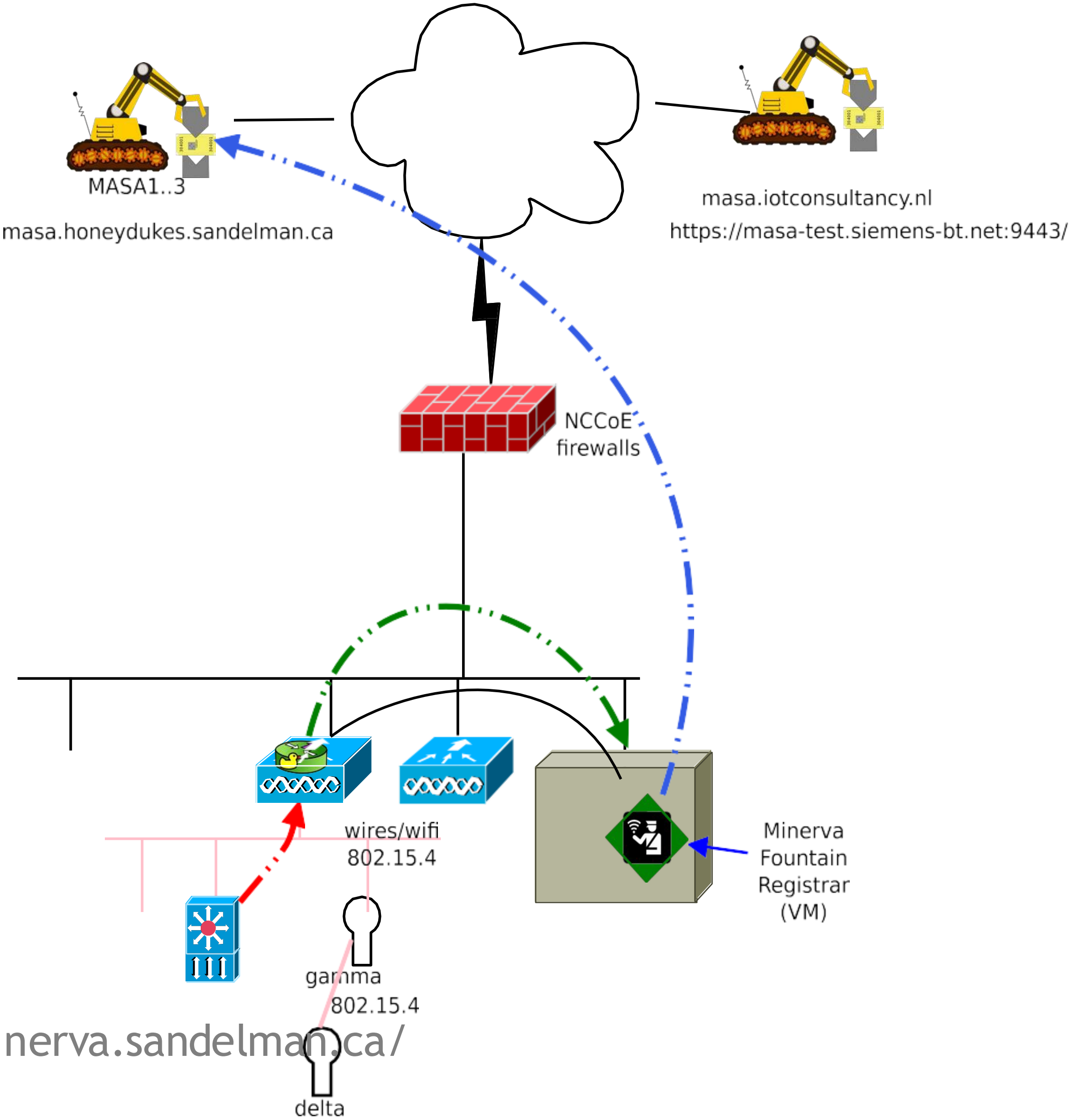


https://minerva.sandelman.ca/

June 2023 – Iteration 2 work

Goals of iteration 2

- Validation of Registrar/Join-Proxy
- Auto-discovery of Join-Proxy by Pledge

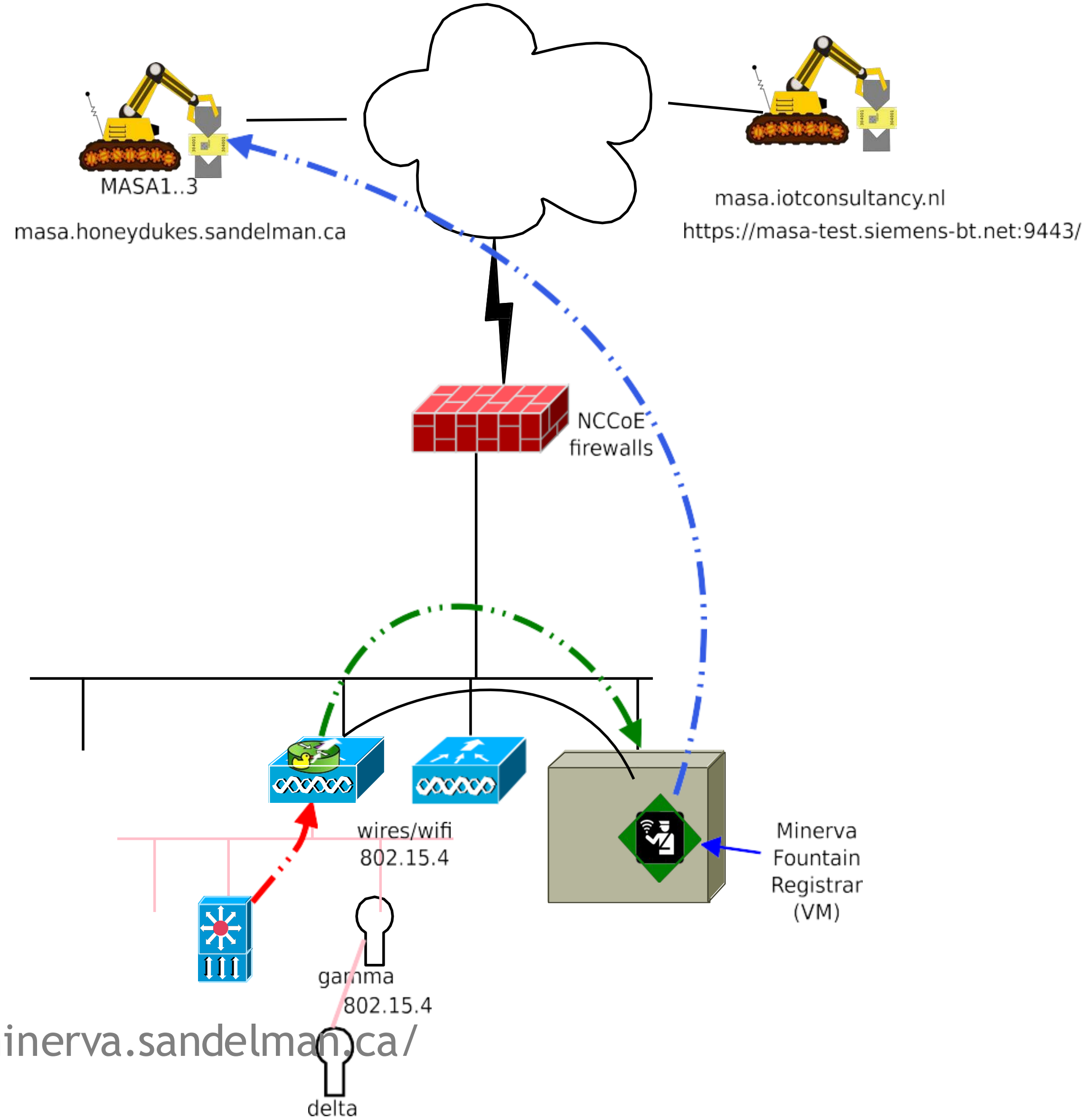


https://minerva.sandelman.ca/

June 2023 – Iteration 3 work

Goals of iteration 3

- Use of WIFI for onboarding



https://minerva.sandelman.ca/

Build 4: Thread and Cloud Onboarding

Brecht Wyseur

SILICON LABS

KUDELSKI IoTHINGS

Trusted Network and Application-Layer Onboarding from Device to Cloud

- **Build 4 Achievements: Seamless Onboarding of IoT Thread Devices**

1. Thread Network Onboarding

   After network onboarding, IoT devices can communicate to the internet via the Boarder Router.

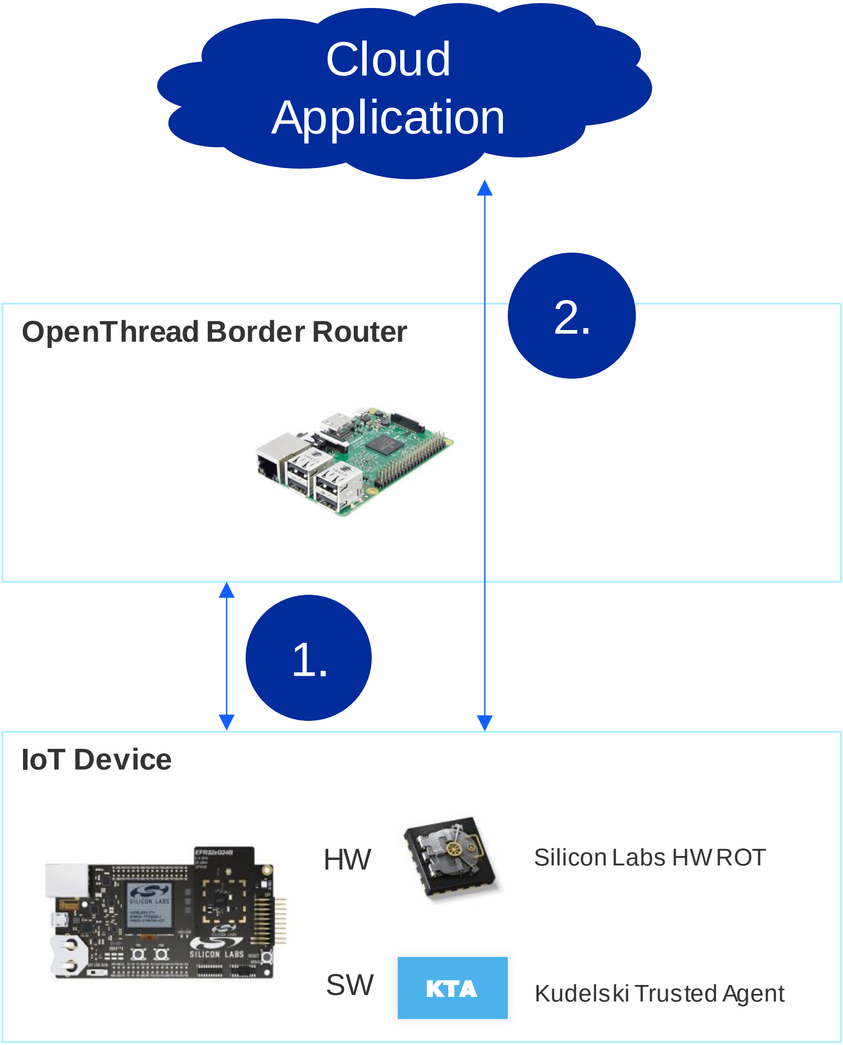
2. Cloud Application-Layer Onboarding

   The lifecycle of the IoT device can be remotely managed – including cloud application onboarding.

- **Easy and Secure**

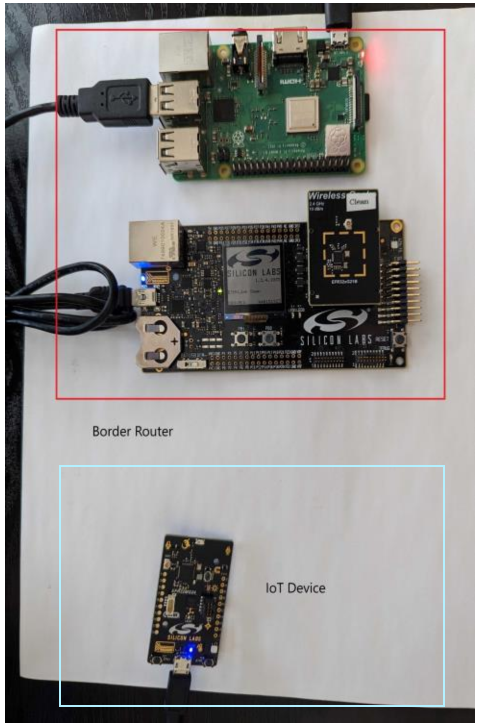
  - End-to-end secure communication, from IoT device to cloud
  - Using Silicon Lab HW Root of Trust: Secure Vault
  - Seamless onboarding: one-time configuration, after which all devices owned by the end-user will be onboarded automatically on the user's Cloud Application.
  - Demonstrated with AWS IoT onboarding
  - Integrated with Silicon Labs Gecko SDK – easy to put in place

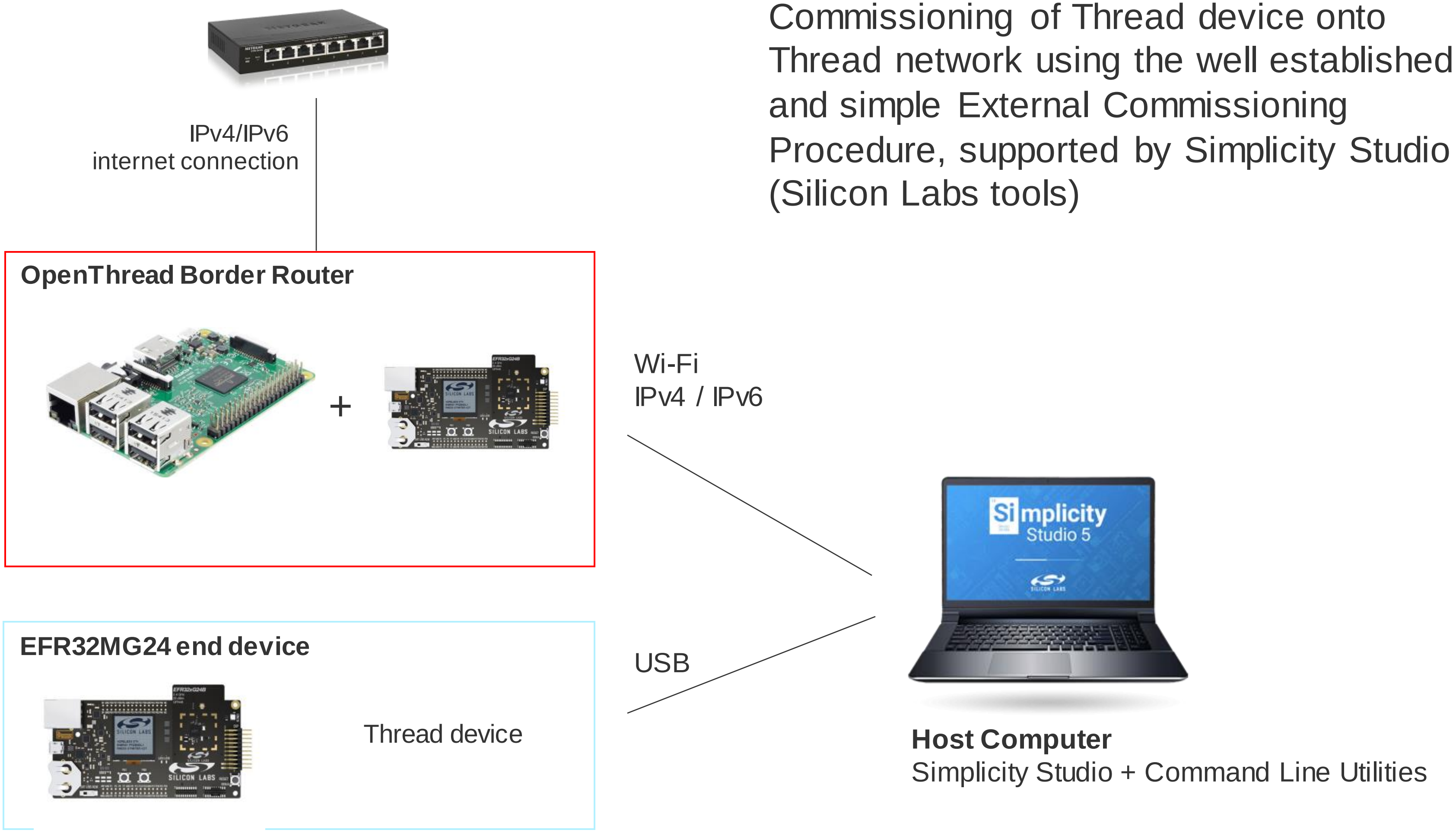
Thanks to Silicon Labs and Kudelski IoT partnership



Network-Layer Onboarding: Simple External Commissioning Procedure

Commissioning of Thread device onto Thread network using the well established and simple External Commissioning Procedure, supported by Simplicity Studio (Silicon Labs tools)





IPv4/IPv6
internet connection

OpenThread Border Router

+

EFR32MG24 end device

Thread device

Wi-Fi
IPv4 / IPv6

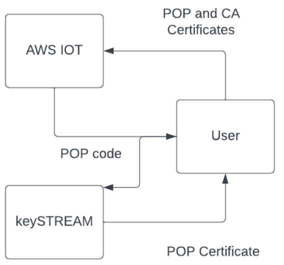
USB

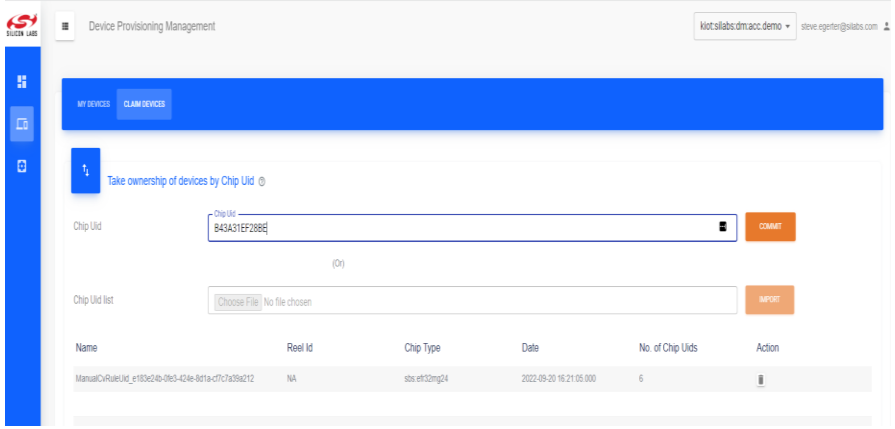
Host Computer
Simplicity Studio + Command Line Utilities

Application-Layer: Automatic Cloud Onboarding (on AWS IoT)

- **Kudelski IoT keySTREAM is a device lifecycle management platform that can manage Silicon Labs SoC credentials**
  - Allows you to manage your device efficiently at scale, through its entire lifecycle
  - Facilitates onboarding using SoC bootstrap credentials

- **One-time Platform Setup**
  - Get your own keySTREAM tenant
  - Setup your keySTREAM onboarding CA and import this in your AWS Account – secured with Proof of Possession.
  - Claim your devices





Take ownership of devices by Chip Uid

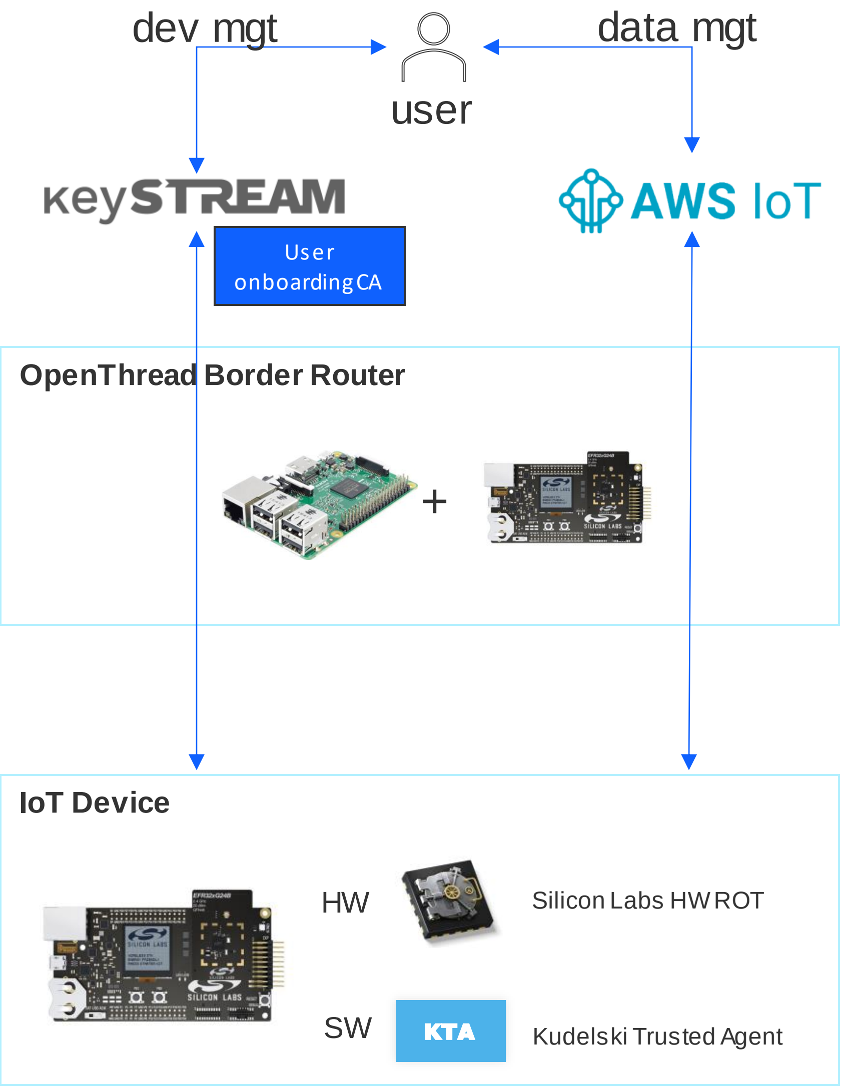
Chip Uid: B43A31EF28BE

(Or)

Chip Uid list: Choose File No file chosen

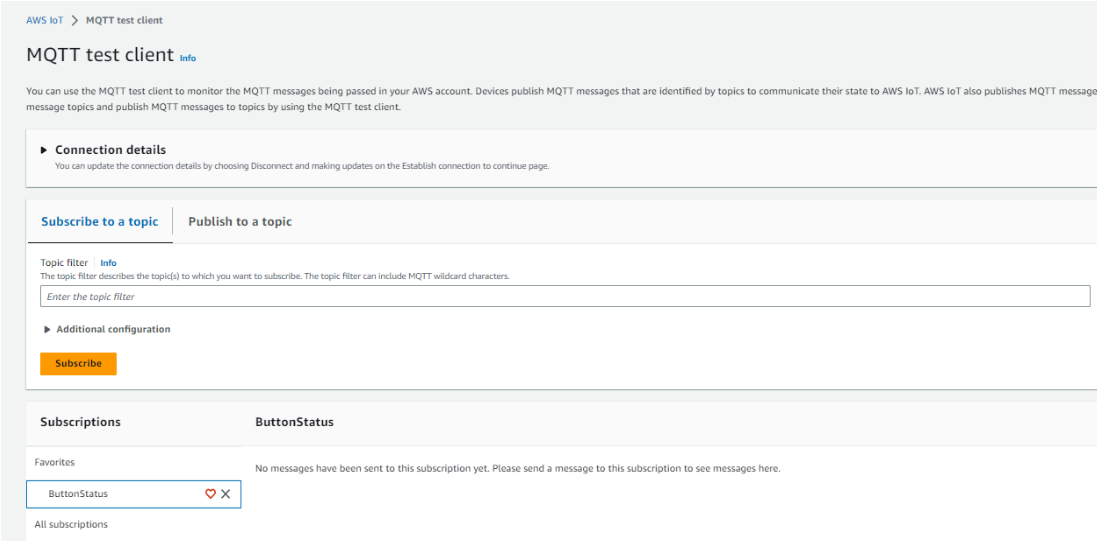
Name	Reel Id	Chip Type	Date	No. of Chip Uids	Action
ManualCvRuleUid_e183e24b-0fe3-424e-8d1a-cf7c7a39a212	NA	sbs:efr32mg24	2022-09-20 16:21:05.000	6	

- **Automatic Onboarding – manage devices at scale**
  - Your devices will automatically onboard and connect to your AWS IoT
  - Secured using SoC bootstrap credentials



Your IoT Devices can now talk securely to the Cloud

- **AWS IOT Speaks MQTT**
  - A light publish/subscribe-based protocol designed for IoT



AWS IoT > MQTT test client

MQTT test client Info

You can use the MQTT test client to monitor the MQTT messages being passed in your AWS account. Devices publish MQTT messages that are identified by topics to communicate their state to AWS IoT. AWS IoT also publishes MQTT message message topics and publish MQTT messages to topics by using the MQTT test client.

▸ Connection details

You can update the connection details by choosing Disconnect and making updates on the Establish connection to continue page.

Subscribe to a topic | Publish to a topic

Topic filter | Info

The topic filter describes the topic(s) to which you want to subscribe. The topic filter can include MQTT wildcard characters.

Enter the topic filter

▸ Additional configuration

Subscribe

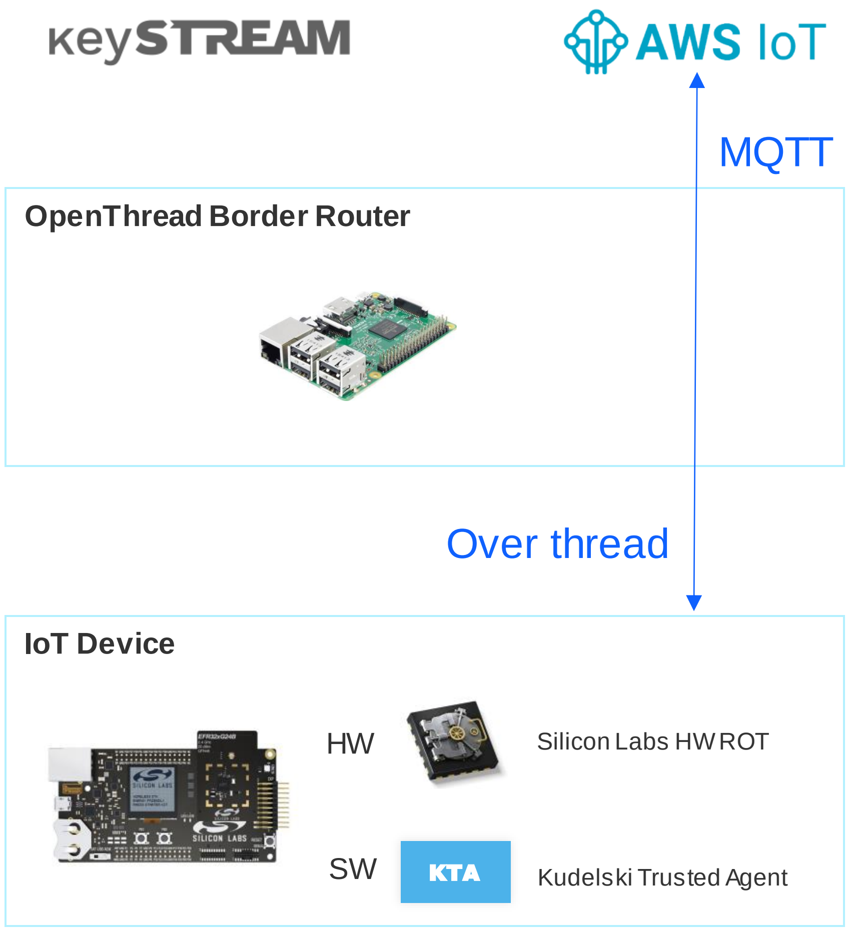
Subscriptions | ButtonStatus

Favorites

ButtonStatus ♡ ✕

All subscriptions

No messages have been sent to this subscription yet. Please send a message to this subscription to see messages here.



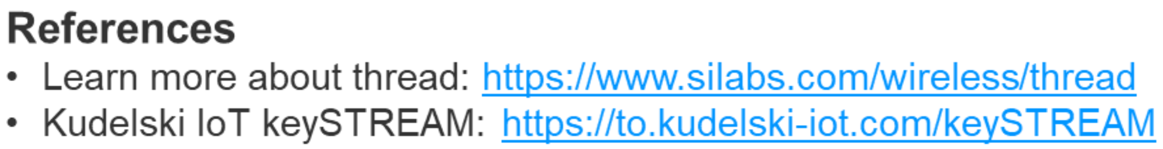
- **Full Capability on Embedded IoT Device**
  - We demonstrate that the IoT Device with the Silicon Labs SoC can run all the software to perform secure communication based on MQTT over Thread to AWS IoT

Thank You

- Brecht Wyseur, Kudelski IoT

Silabs.com

Kudelski-iot.com



References

- Learn more about thread: https://www.silabs.com/wireless/thread
- Kudelski IoT keySTREAM: https://to.kudelski-iot.com/keySTREAM

Trusted IoT Device Network-Layer Onboarding and Lifecycle Management

Build 5:
BRSKI, NquiringMinds

Nick Allott

nquringminds

Trusted IOT Lifecycle

Big Picture – why is this important

nquiringminds

Usability

- Managing IOT devices hard, very difficult to use

Security fixes

- Current conventions, have serious flaws (e.g browser)

Security improvements

- Opportunity to improve status quo, though best practice and modern methods

Supply chain

- Better integrated supply chain security

Scalability/Efficiency

- Onboarding enterprise devices at scale, zero touch methods

Business model innovation

- New management methods open up new business model opportunities and better integrated security

Continuous assurance

- Shift from a one-off check to continuous assurance. Embodies zero trust concepts

Objectives

Build 5

Demonstrate BRSKI over WIFI – Scenario 1

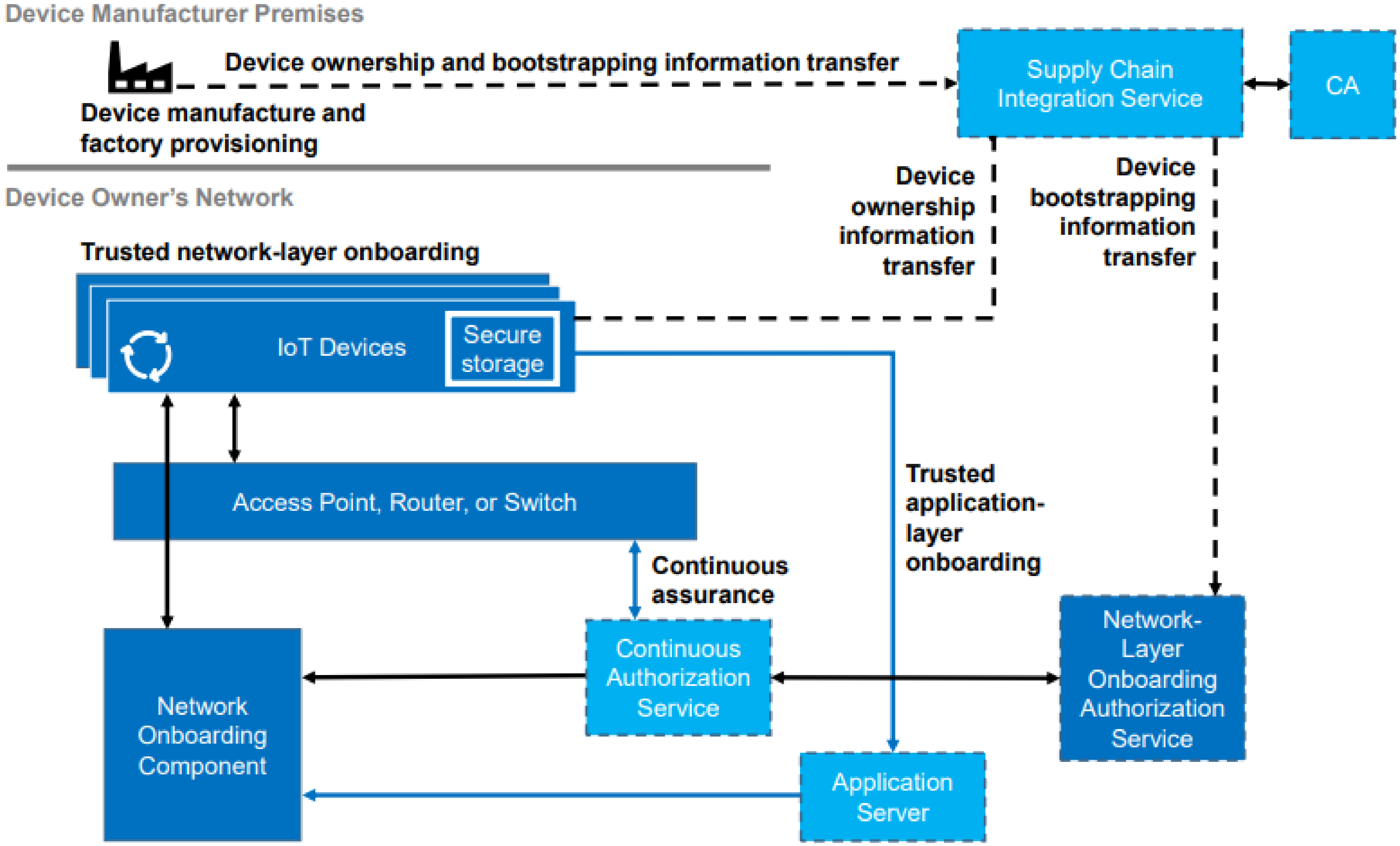
- Scenario 1: Trusted Network-Layer Onboarding
- Demonstrate the WIFI flows in detail
- Interoperability testing across builds - and factory flows

Demonstrate BRSKI over WIFI – Advanced Scenarios

- Scenario 2: Trusted Application-Layer Onboarding (Browser)
- Scenario 3: Re-Onboarding a Device
- Scenario 4: Ongoing Device Validation

Develop Continuous Assurance

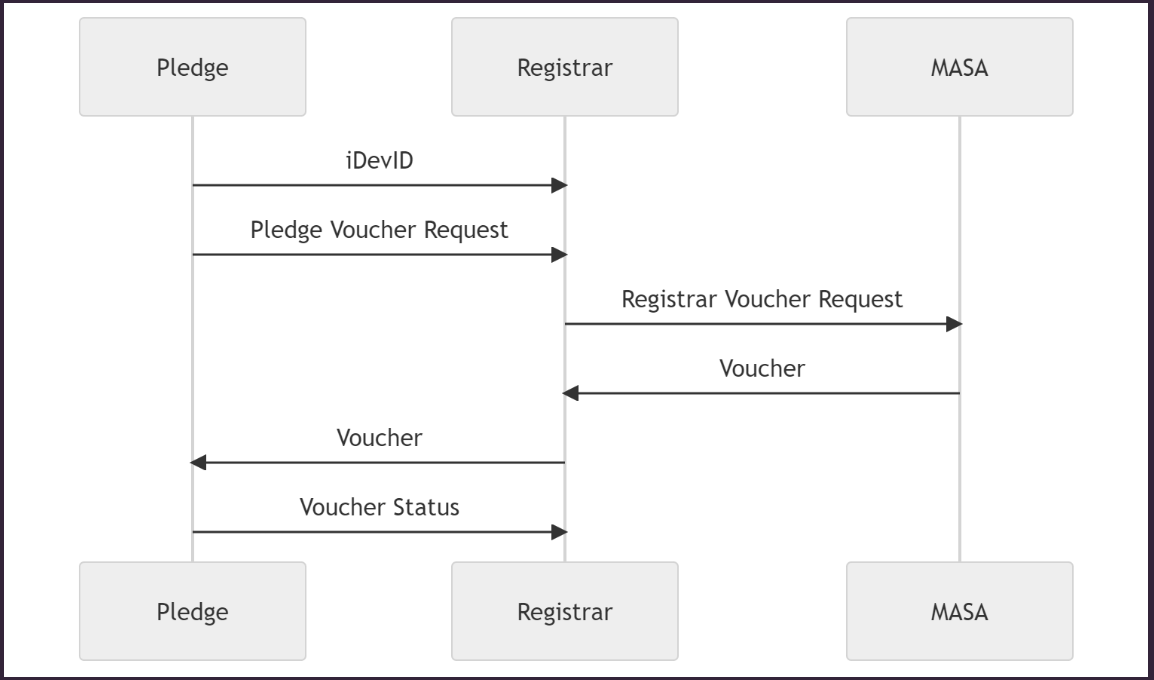
- Scenario 5: Establishment and Maintenance of Credential and Device Security Posture Throughout the Lifecycle
- Continuous assurance as a flexible extensible method of achieving the advanced scenarios
- Identify interoperability opportunities across build



Device Manufacturer Premises
Device ownership and bootstrapping information transfer
Device manufacture and factory provisioning
Supply Chain Integration Service
CA
Device Owner's Network
Device ownership information transfer
Device bootstrapping information transfer
Trusted network-layer onboarding
IoT Devices
Secure storage
Access Point, Router, or Switch
Continuous assurance
Trusted application-layer onboarding
Network Onboarding Component
Continuous Authorization Service
Network-Layer Onboarding Authorization Service
Application Server

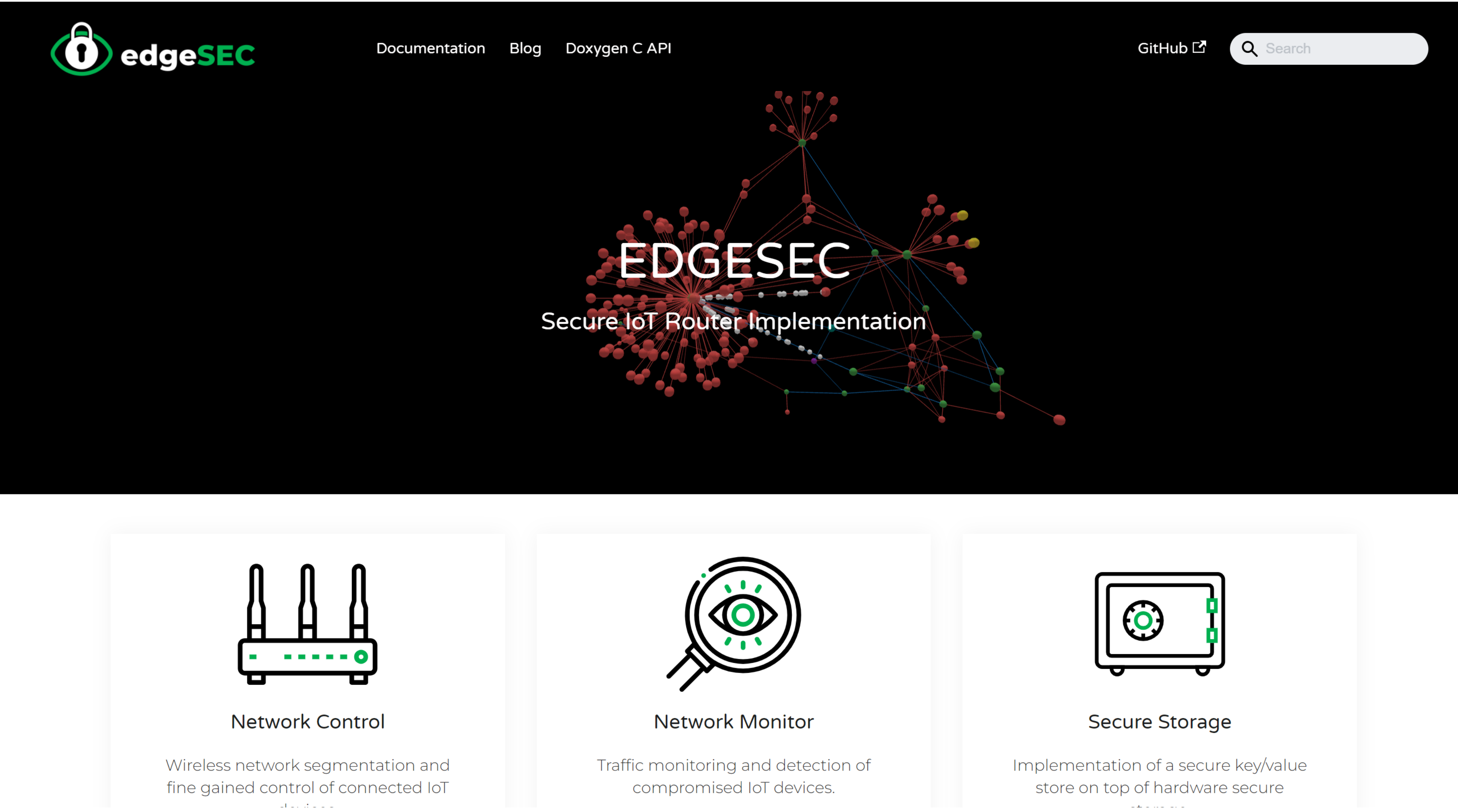
EXAMPLE

Policy variants



Examples of policy

- Manufacturer approved by network owner
- Device is from manufacturer (no record of instance)
- Device is from manufacturer (with record of instance)
- DeviceID is approved by network owner
- Device presents attestation voucher approved by manufacturer
- Device instance is certified
- Device type is certified
- Device behaviour is in network perimeter
- Active vulnerabilities are below threshold



EDGESEC

Secure IoT Router Implementation

Network Control

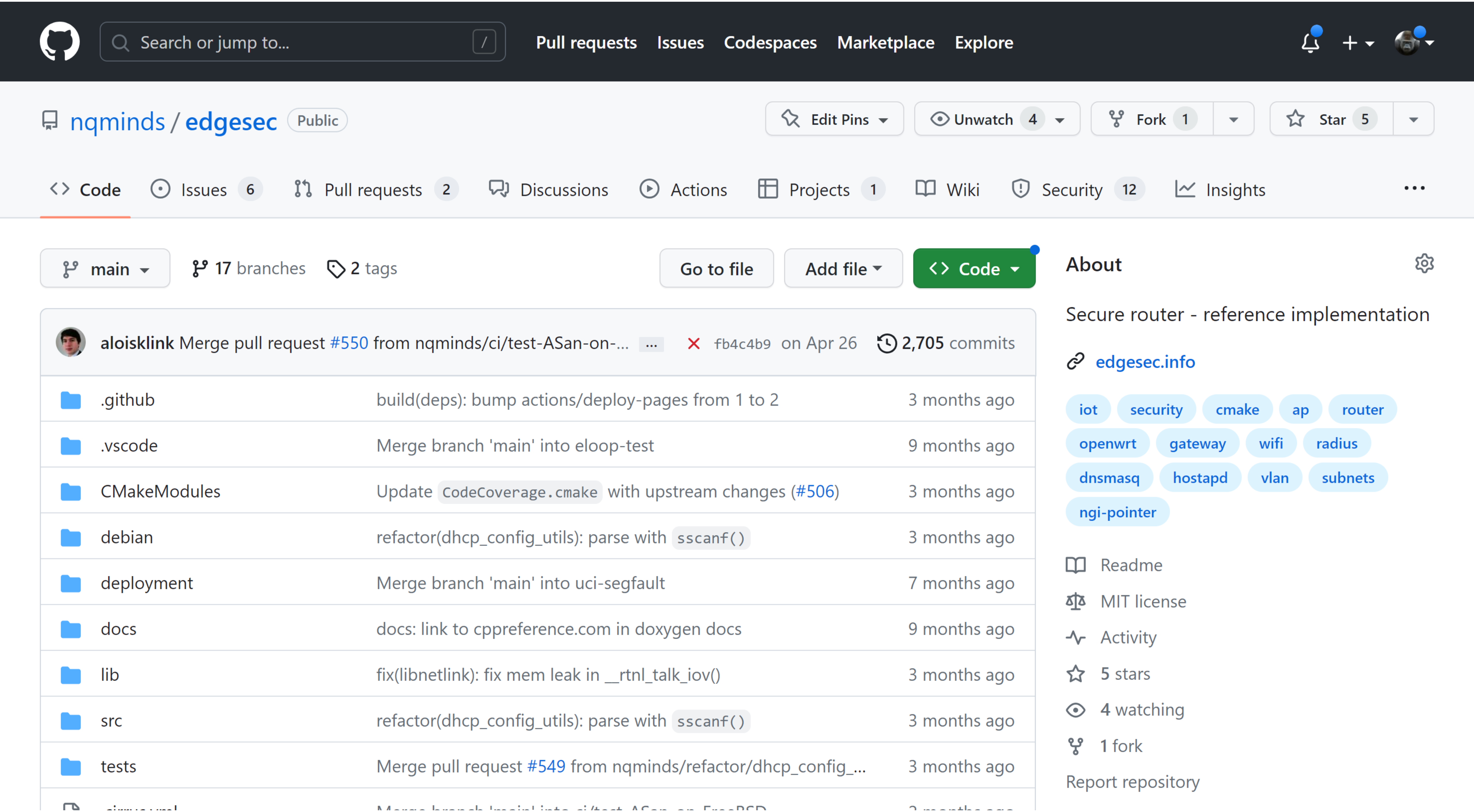
Wireless network segmentation and fine gained control of connected IoT devices.

Network Monitor

Traffic monitoring and detection of compromised IoT devices.

Secure Storage

Implementation of a secure key/value store on top of hardware secure storage.



nqminds / edgesec Public

17 branches 2 tags

aloisklink Merge pull request #550 from nqminds/ci/test-ASan-on-... ... ✗ fb4c4b9 on Apr 26 2,705 commits

.github	build(deps): bump actions/deploy-pages from 1 to 2	3 months ago
.vscode	Merge branch 'main' into eloop-test	9 months ago
CMakeModules	Update `CodeCoverage.cmake` with upstream changes (#506)	3 months ago
debian	refactor(dhcp_config_utils): parse with `sscanf()`	3 months ago
deployment	Merge branch 'main' into uci-segfault	7 months ago
docs	docs: link to cppreference.com in doxygen docs	9 months ago
lib	fix(libnetlink): fix mem leak in __rtnl_talk_iov()	3 months ago
src	refactor(dhcp_config_utils): parse with `sscanf()`	3 months ago
tests	Merge pull request #549 from nqminds/refactor/dhcp_config_...	3 months ago
.cirrus.yml	Merge branch 'main' into ci/test-ASan-on-FreeBSD	3 months ago

About

Secure router - reference implementation

edgesec.info

iot security cmake ap router openwrt gateway wifi radius dnsmasq hostapd vlan subnets ngi-pointer

Readme

MIT license

Activity

5 stars

4 watching

1 fork

Report repository

Open source assets

https://edgesec.info/
https://github.com/nqminds/edgesec

Questions

nick@nquiringminds.com
Nick Allott

NCCoE IoT Onboarding

Factory Provisioning Use-Case: Goals & Demo

SEAL SQ semiconductors + quantum

- A WISeKey company

Sandelman Software Works

SEALSQ
- Steve Clark
  Security Technologist

Sandelman Software Works
- Michael Richardson
  Chief Scientist

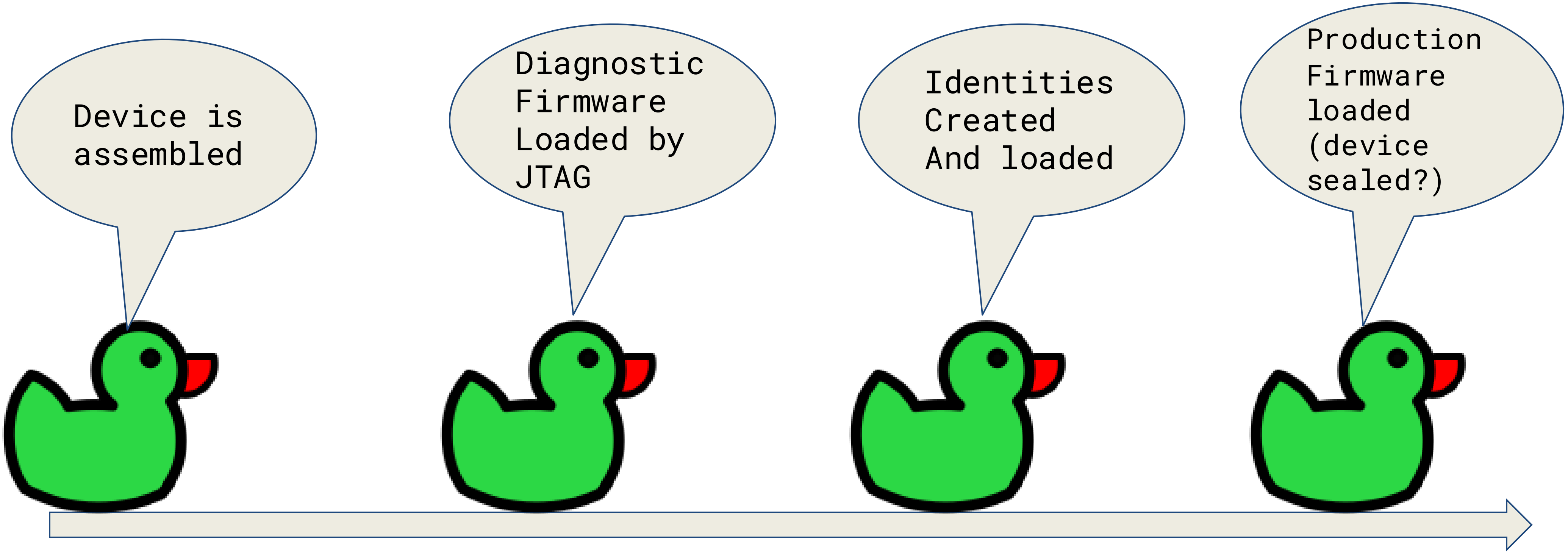
- 01 November, 2023

Goals of the Factory Provisioning Use-Case

- Build itself:
  - Generate private key, with associated public key enrolled into database, to produce certificate or DPP (QR)code

- Experimental Goals
  - Advocate an identity of devices be provisioned by the manufacturer
  - Document one or more flows involving BRSKI, DPP, (Thread) where a key is generated (in a secure element), and enrolled
  - Identify options (incl. those not implemented), and give them (public) names

Model of how Factory Provisioning Use-Case might Work



Device is assembled

Diagnostic Firmware Loaded by JTAG

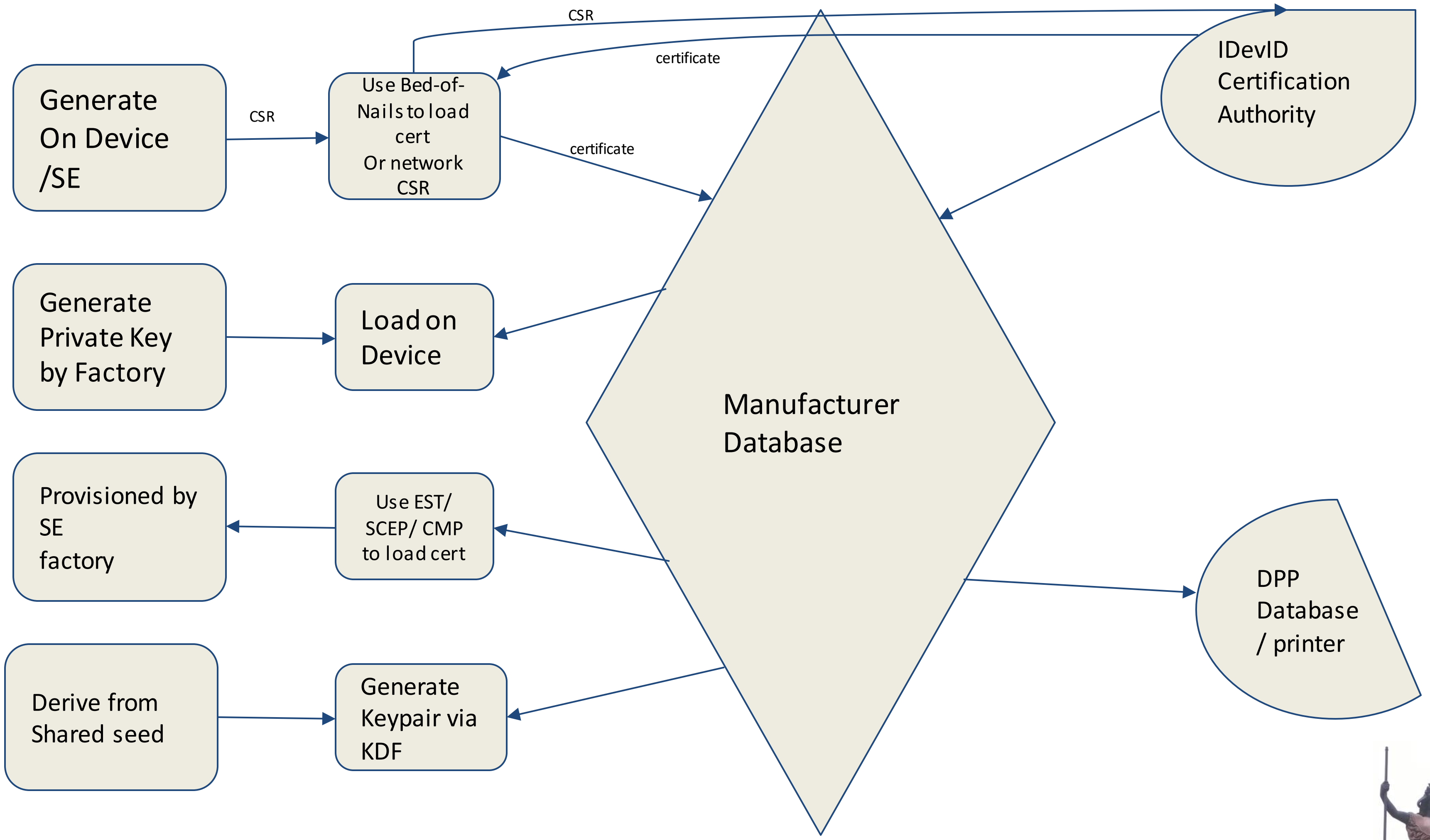
Identities Created And loaded

Production Firmware loaded (device sealed?)

Assembly Line

https://en.wikipedia.org/wiki/Bed_of_nails_tester

Different Approaches to Provisioning Identities



Generate On Device /SE
CSR
Use Bed-of-Nails to load cert Or network CSR
CSR
certificate
certificate
IDevID Certification Authority
Generate Private Key by Factory
Load on Device
Manufacturer Database
Provisioned by SE factory
Use EST/ SCEP/ CMP to load cert
DPP Database / printer
Derive from Shared seed
Generate Keypair via KDF

SEALSQ is a WISeKey Company

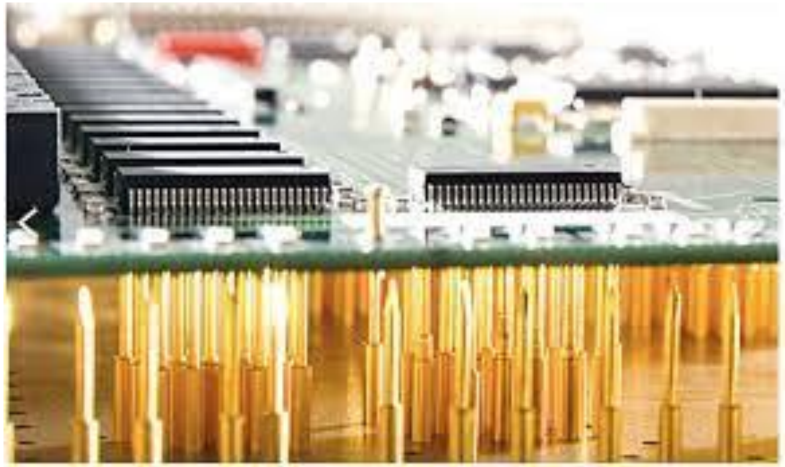
SEAL SQ semiconductors + quantum

The Demo

- **Limitations:**
  - ○ We do not have a factory, or bed-of-nails interface
  - ○ Firmware loading process for RPI involved humans manipulating SDcards

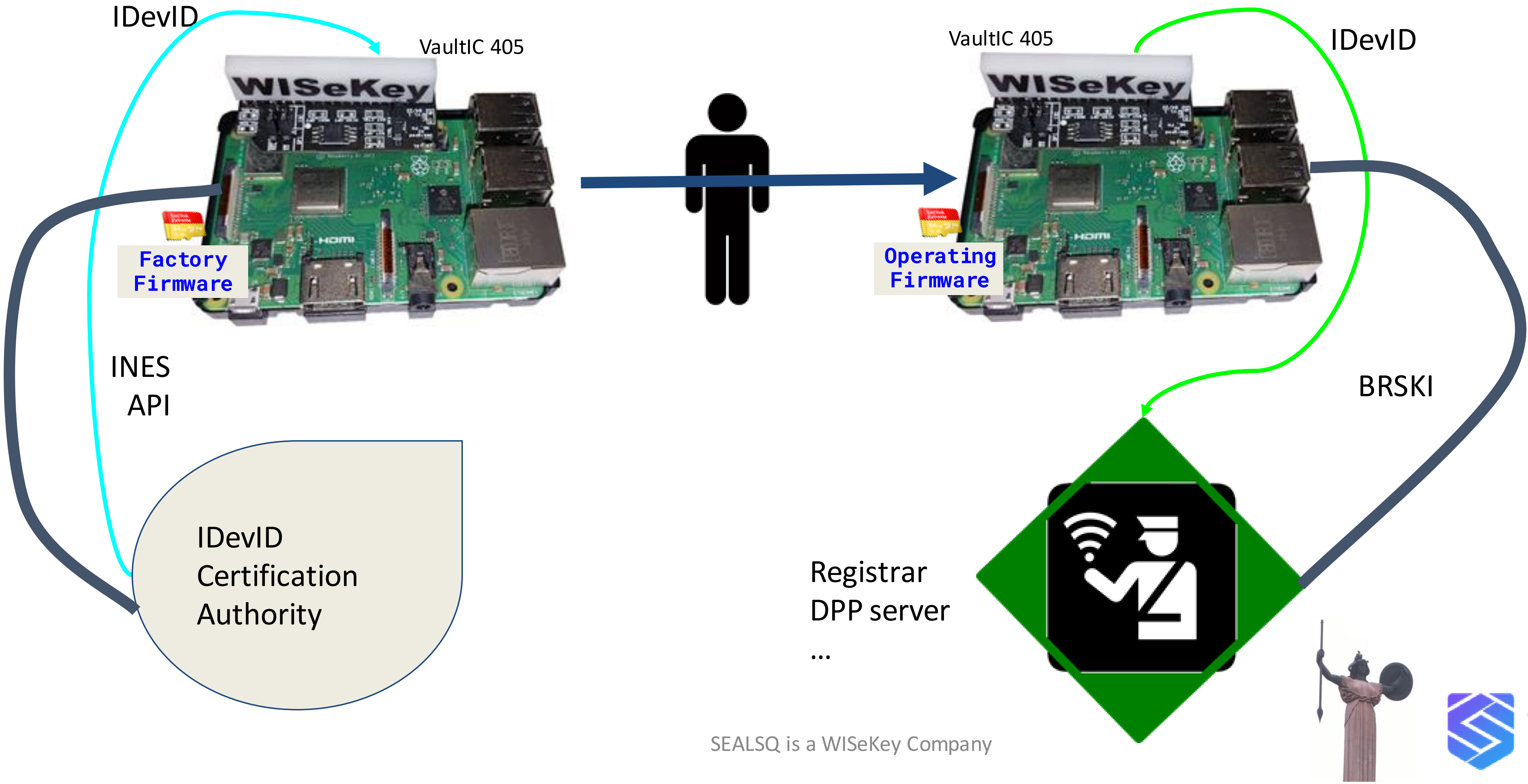
- **Implementation**
  - ○ Pre-provision a secure element with an immutable Identity
  - ○ Install the secure element on an IoT edge device to establish the platform hardware root of trust and Identity

- **Technologies**
  - ○ Raspberry Pi Platform
  - ○ VaultIC 405 Secure Element
  - ○ INeS Certificate Management System API
  - ○ INeS-Hosted Certificate Authority



https://en.wikipedia.org/wiki/Bed_of_nails_tester

Overview Factory Provisioning Use-Case Demo



IDevID

VaultIC 405

Factory Firmware

INES API

IDevID Certification Authority

VaultIC 405

IDevID

Operating Firmware

BRSKI

Registrar
DPP server
…

SEAL SQ semiconductors + quantum

Thank You

SEALSQ semiconductors

Audience Q & A

Please submit questions to our panelists using the WebEx chat box.

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Thank you for joining us!

Visit our project page for Draft NIST SP 1800-36:

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

nccoe.nist.gov

@NISTcyber

iot-onboarding@nist.gov