Welcome to the National Cybersecurity Center of Excellence

Trusted IoT Onboarding: Updates to DRAFT NIST SP 1800-36

Wednesday, July 10th, 2024 | 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

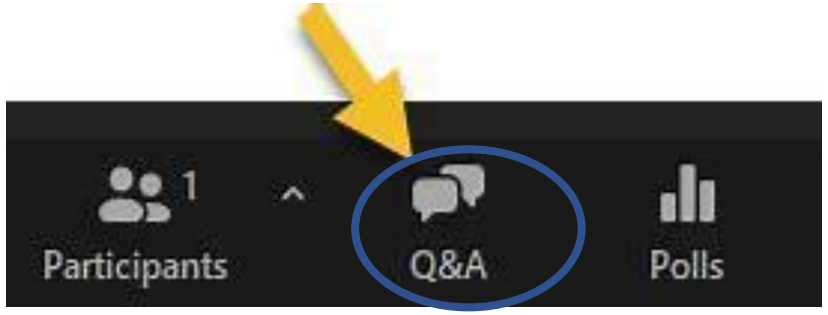
Time (ET)	Session	Speaker(s)
10:00–10:05 a.m.	Welcome and Introduction	• Tim McBride, Deputy Director, NIST NCCoE • Paul Watrobski, Principal Investigator, NIST NCCoE
10:05–10:20 a.m.	Project Overview • Cybersecurity problem, general build architecture, and publication status of NIST SP 1800-36	• Paul Watrobski, Principal Investigator, NIST NCCoE
10:20–10:30 a.m.	Build 4 • Discussion on Updates to Trusted Network-Layer Onboarding with the Thread Protocol	• Brecht Wyseur, Senior Product Manager and Product Strategy, Kudelski IoT
10:30–10:40 a.m.	Build 5 • Discussion on Trusted Network-Layer Onboarding with BRSKI over Wi-Fi	• Nick Allott, CEO, NquiringMinds
10:40–10:50 a.m.	Build 6 • Discussion on Updates to Factory Provisioning	• Steve Clark, Security Technologist, SEALSQ • Michael Richardson, Chief Scientist, Sandelman Software Works

Agenda cont.

Time (ET)	Session	Speaker(s)
10:50–10:58 a.m.	Build 1 • Discussion on Trusted Network-Layer Onboarding with Wi-Fi Easy Connect	• Dan Harkins, Fellow, HPE Aruba
10:58–11:06 a.m.	Build 2 • Discussion on Trusted Network-Layer Onboarding with Wi-Fi Easy Connect	• Andy Dolan, Senior Security Engineer, CableLabs • Craig Pratt, Lead Software Engineer, CableLabs • Darshak Thakore, Principal Architect, CableLabs
11:06–11:25 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

Recording Notice and Q&A

- This event is being recorded.
- For questions and comments, please use the **Q&A feature**. We will address all questions after the session presentations. Chat has been disabled.



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

Welcome and Introductory Remarks

Tim McBride, Deputy Director, NIST NCCoE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

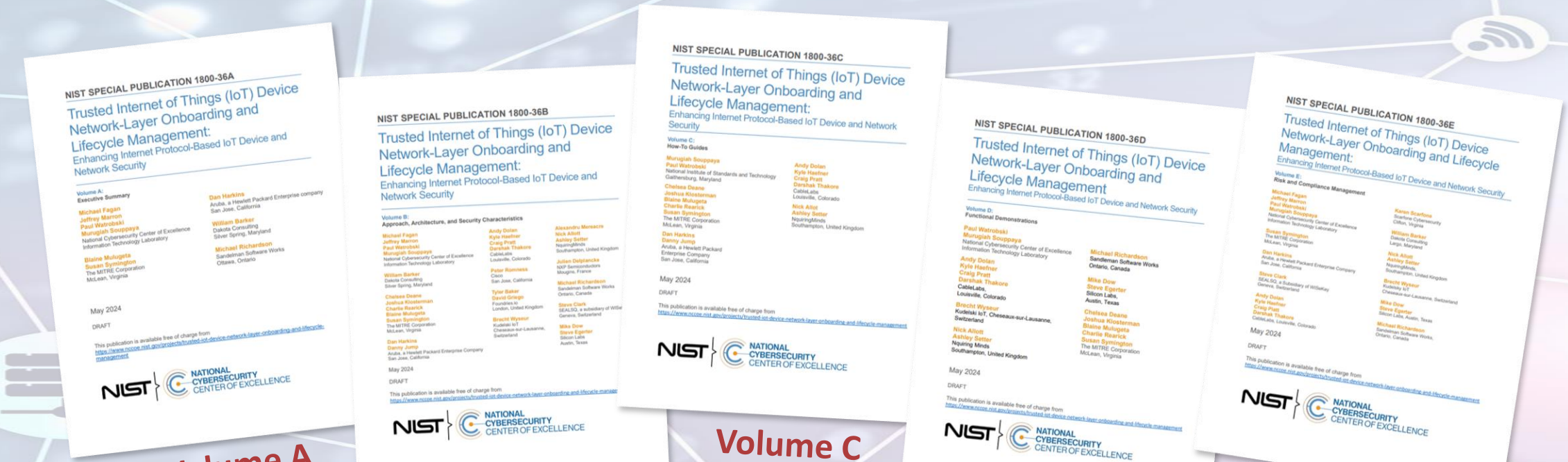
Project Overview

Paul Watrobski, Principal Investigator, NIST NCCoE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SP 1800-36 Practice Guide

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



Volume A
Executive Summary

Volume B
Approach & Architecture

Volume C
How-To Guide

Volume D
Functional Demonstrations

Volume E
Risk & Compliance Management

Final Draft (May 2024)

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

Trusted IoT Network-Layer Onboarding: Objective

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- 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

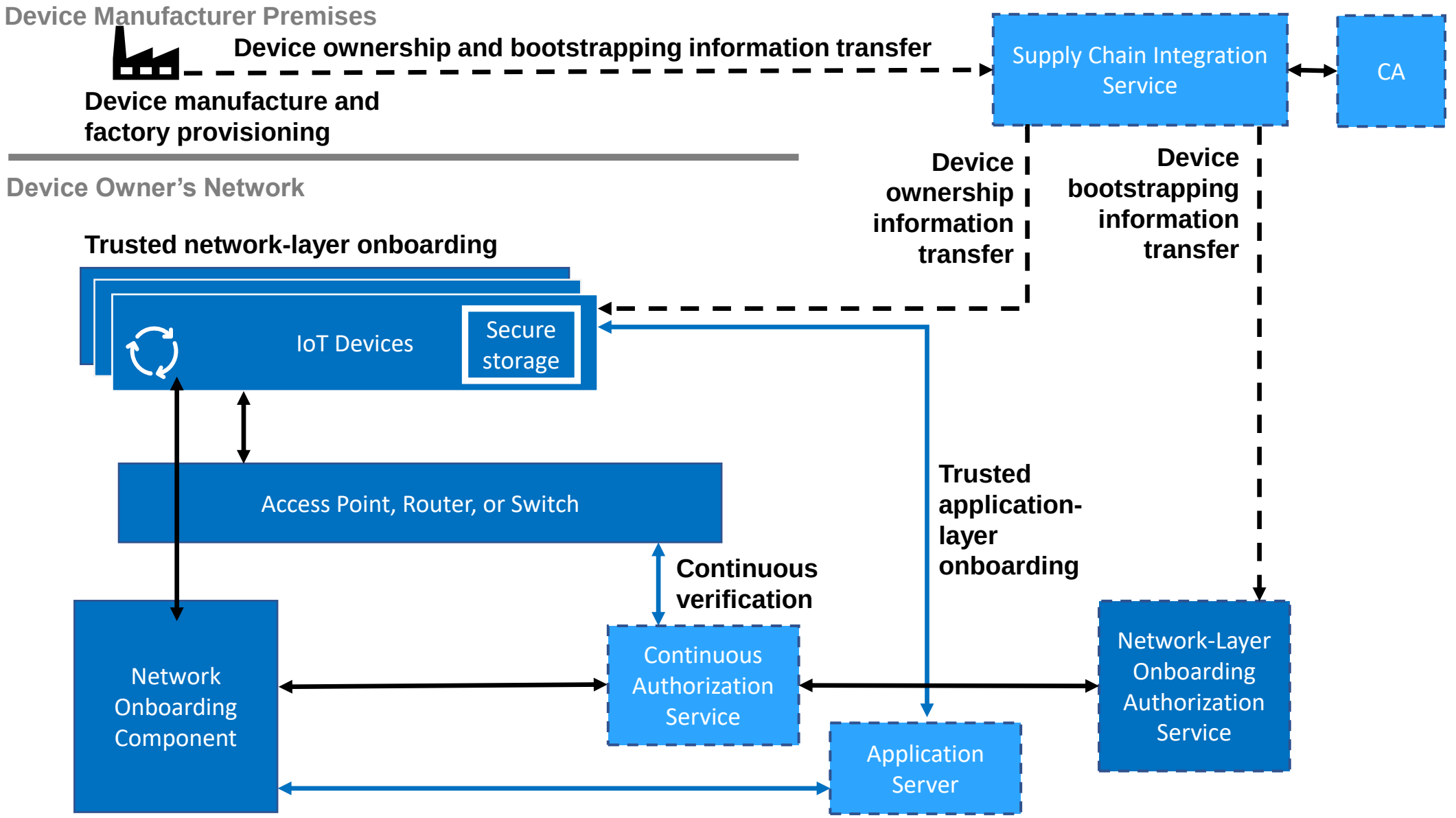
Sources: Statista: • Number of connected devices worldwide 2030 | Statista (38.6 billion)
International Data Corporation (IDC): 41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025 - Help Net Security (41.6 billion)

Trusted IoT Network-Layer Onboarding: Scope

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- *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



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

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- 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
- 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
- Build 3: Bootstrapping Remote Key Infrastructure (BRSKI) Protocol, Sandelman Software Works
  - Collaborators: Sandelman Software Works (Build Champion), NXP Semiconductors, SEALSQ, 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
- **Factory Provisioning Use-Case (cross-build application)**
  - Collaborators: Aruba, an HPE Company, Sandelman Software Works, SEALSQ

Collaborators

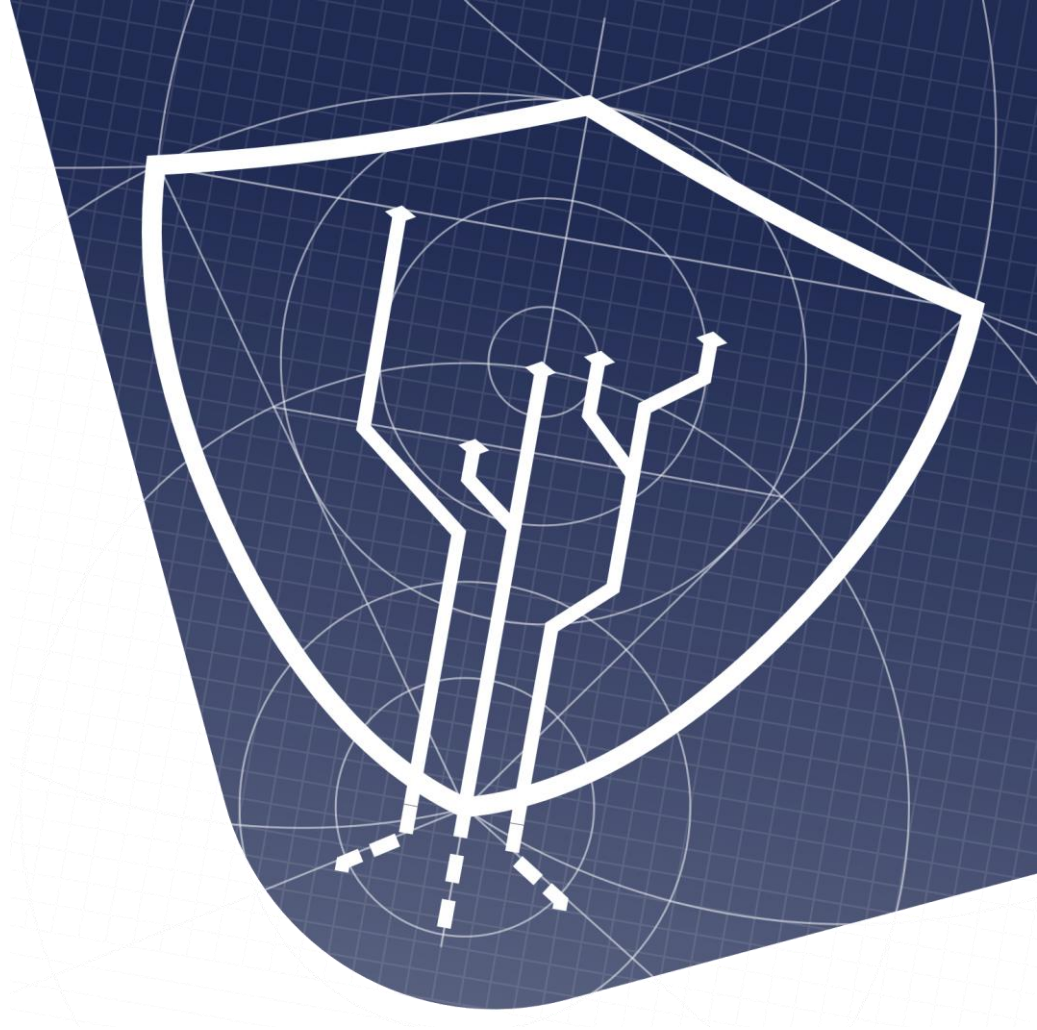
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

How to Get Involved

- The comment period for Draft NIST SP 1800-36 ends at **11:59 PM (ET) on July 30, 2024**.
- Read the draft, comment, and/or join our Community of Interest by visiting the **NCCoE Trusted IoT Onboarding webpage** at nccoe.nist.gov.
- Email all questions, comments, and feedback to our team at iot-onboarding@nist.gov.

KUDELSKI IOT

SILICON LABS



Build 4 – Thread and Cloud Onboarding

Brecht Wyseur, Senior Product Manager and Product Strategy

Kudelski IoT

Trusted Network and Application Layer Onboarding

Build 4 achievements: seamless onboarding of IoT Thread Devices

1. Thread **Network-layer** onboarding

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

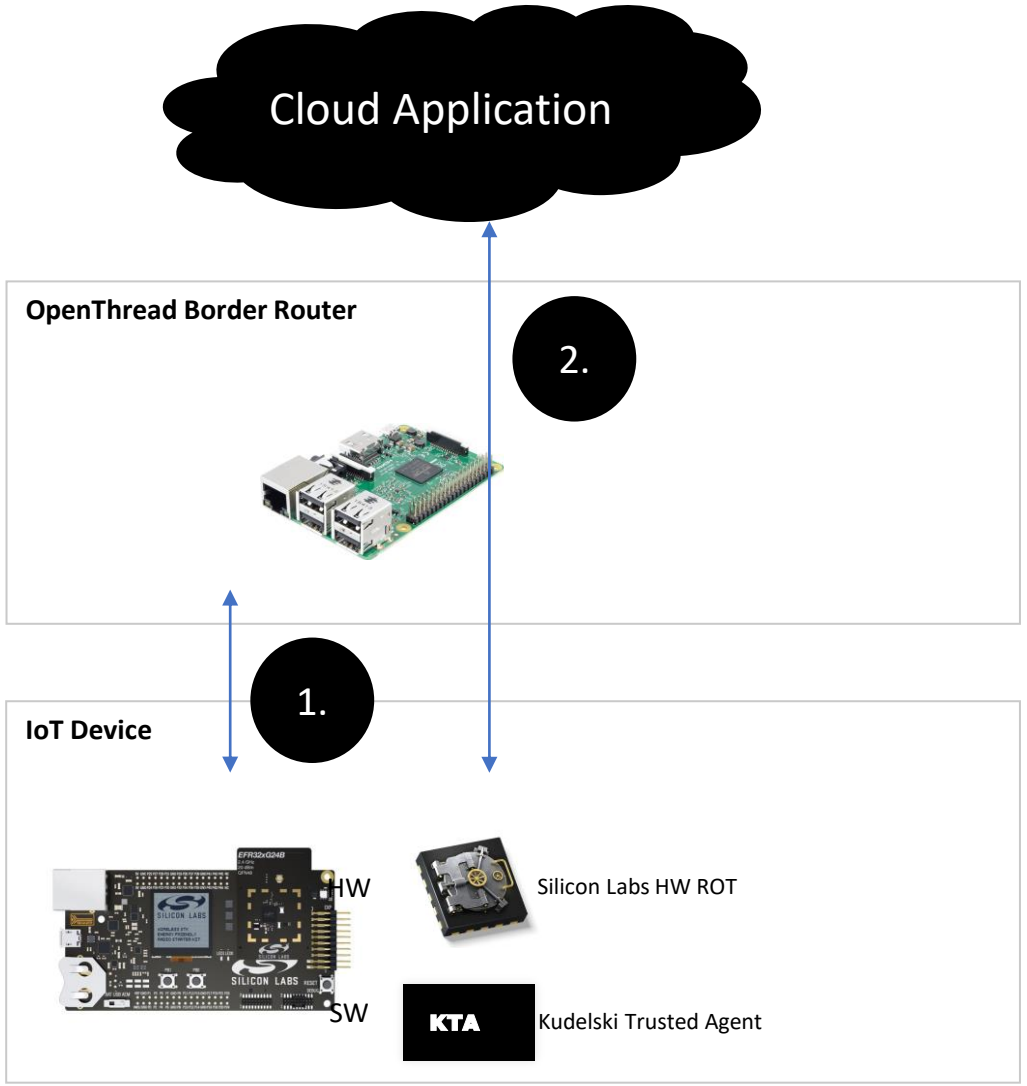
2. Cloud **application-layer** onboarding

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

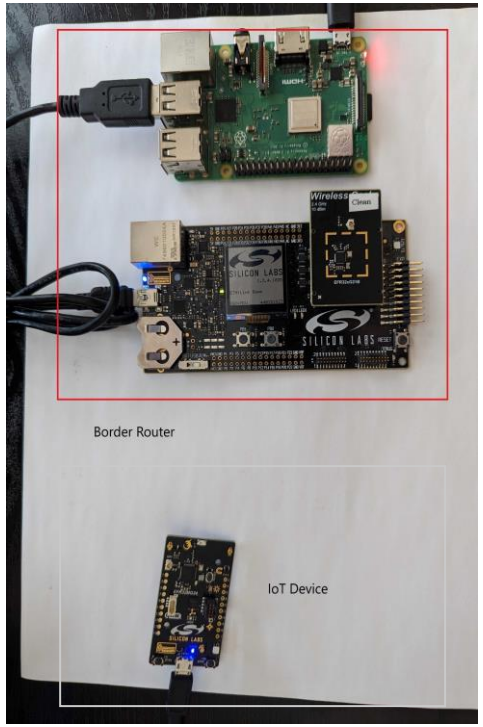
Easy and secure, from chip to cloud

- 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



IPv4/IPv6
internet connection

OpenThread Border Router

+

EFR32MG24 end device

Thread device

Wi-Fi
IPv4 / IPv6

USB

Host Computer
Simplicity Studio + Command Line Utilities

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

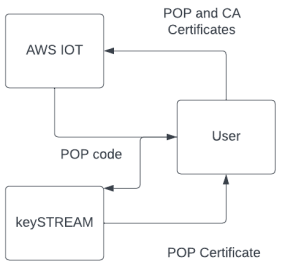
Application-Layer: Automatic Cloud Onboarding

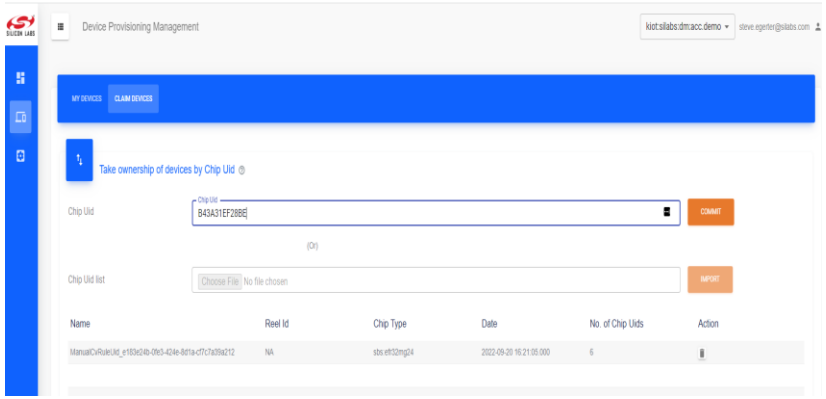
Kudelski IoT keySTREAM is a device lifecycle management platform that can manage Silicon Labs SoC credentials

- Allows you to manage your device efficiently at scale, through its entire lifecycle
- Facilitates onboarding using SoC bootstrap credentials

One-time platform setup

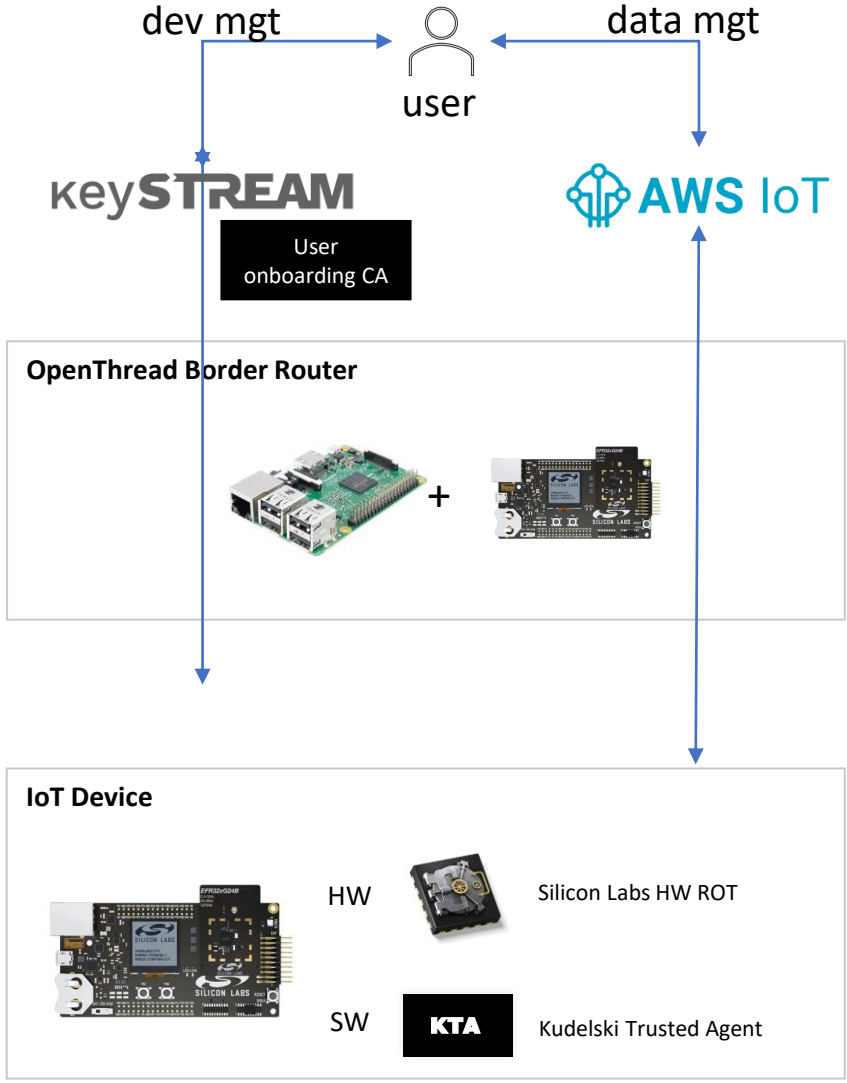
- Get your own keySTREAM tenant
- Setup your keySTREAM onboarding CA and import this in your AWS Account – secured with Proof of Possession.
- Claim your devices





Automatic onboarding – manage devices at scale

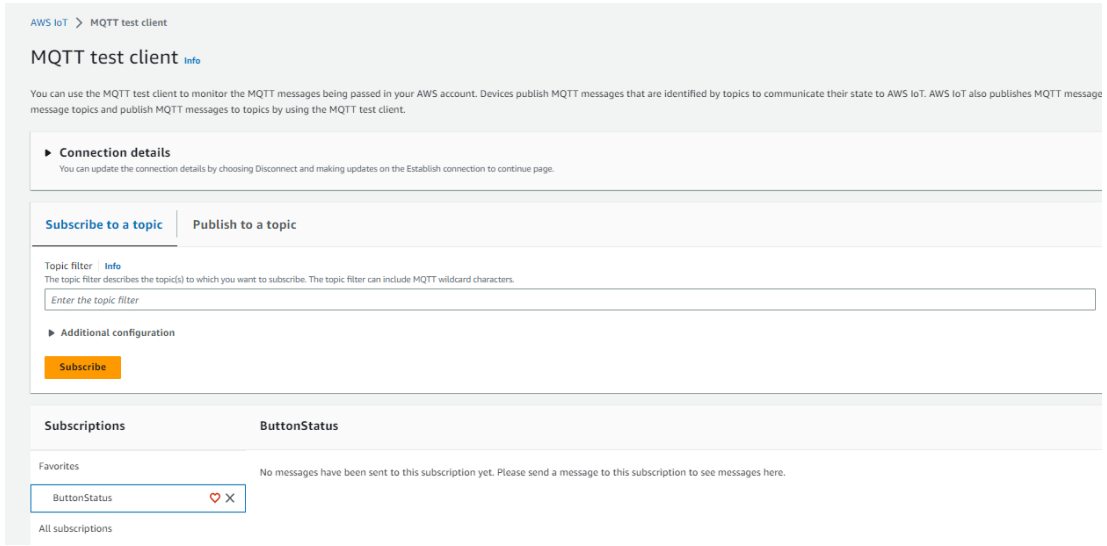
- Your devices will automatically onboard and connect to your AWS IoT
- Secured using SoC bootstrap credentials



Your IoT Devices can now talk securely to the cloud

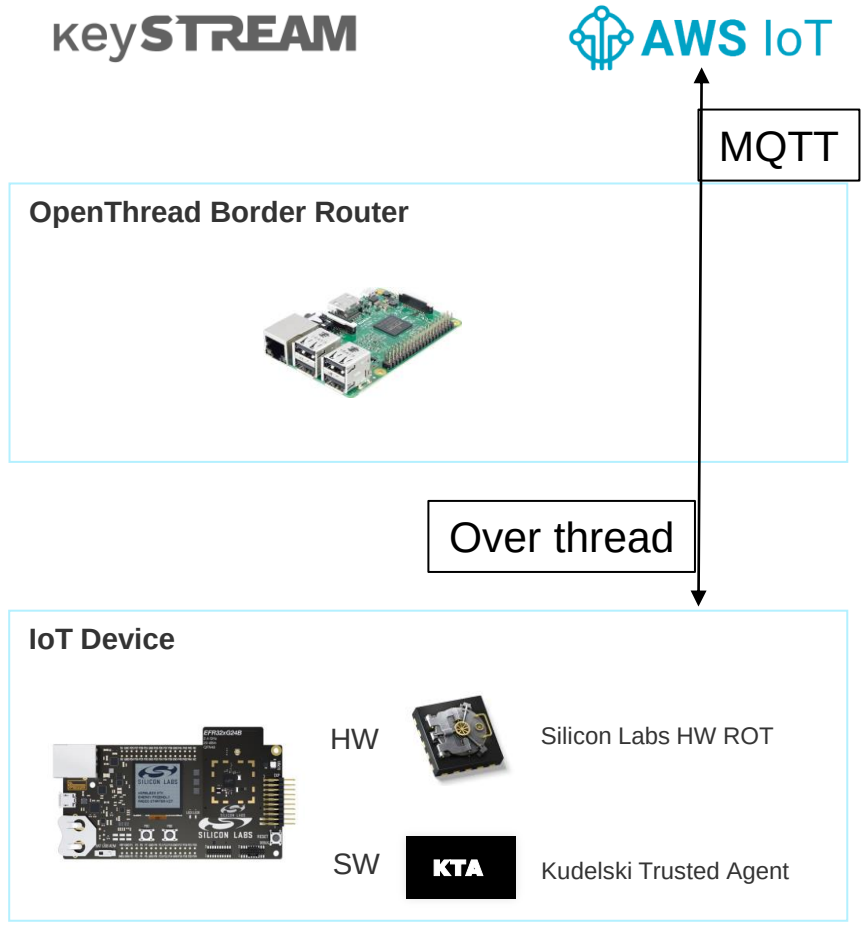
AWS IOT Speaks MQTT

- A light publish/subscribe-based protocol designed for IoT



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@nagra.com

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

BRSK over WIFI

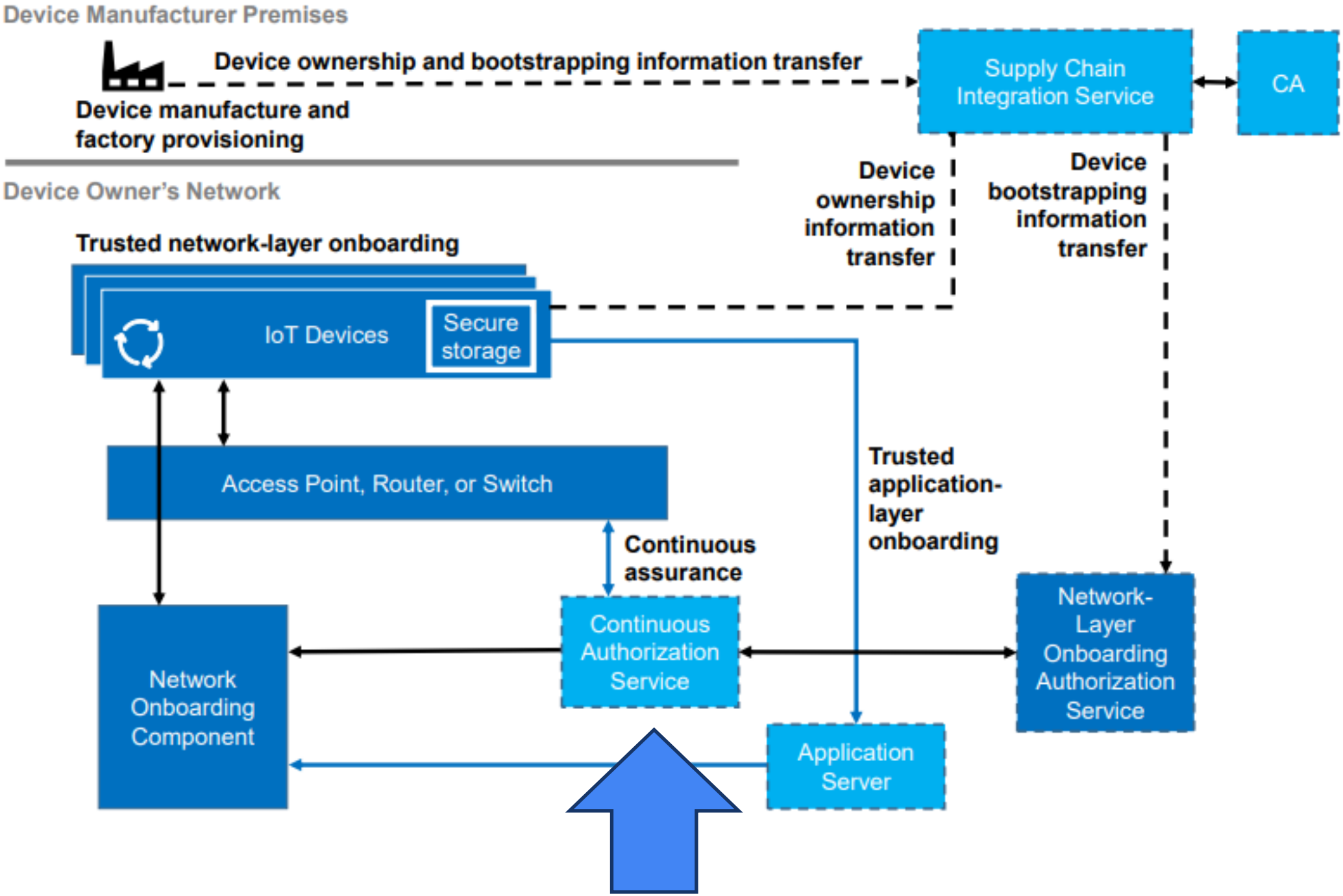
Nick Allott, CEO

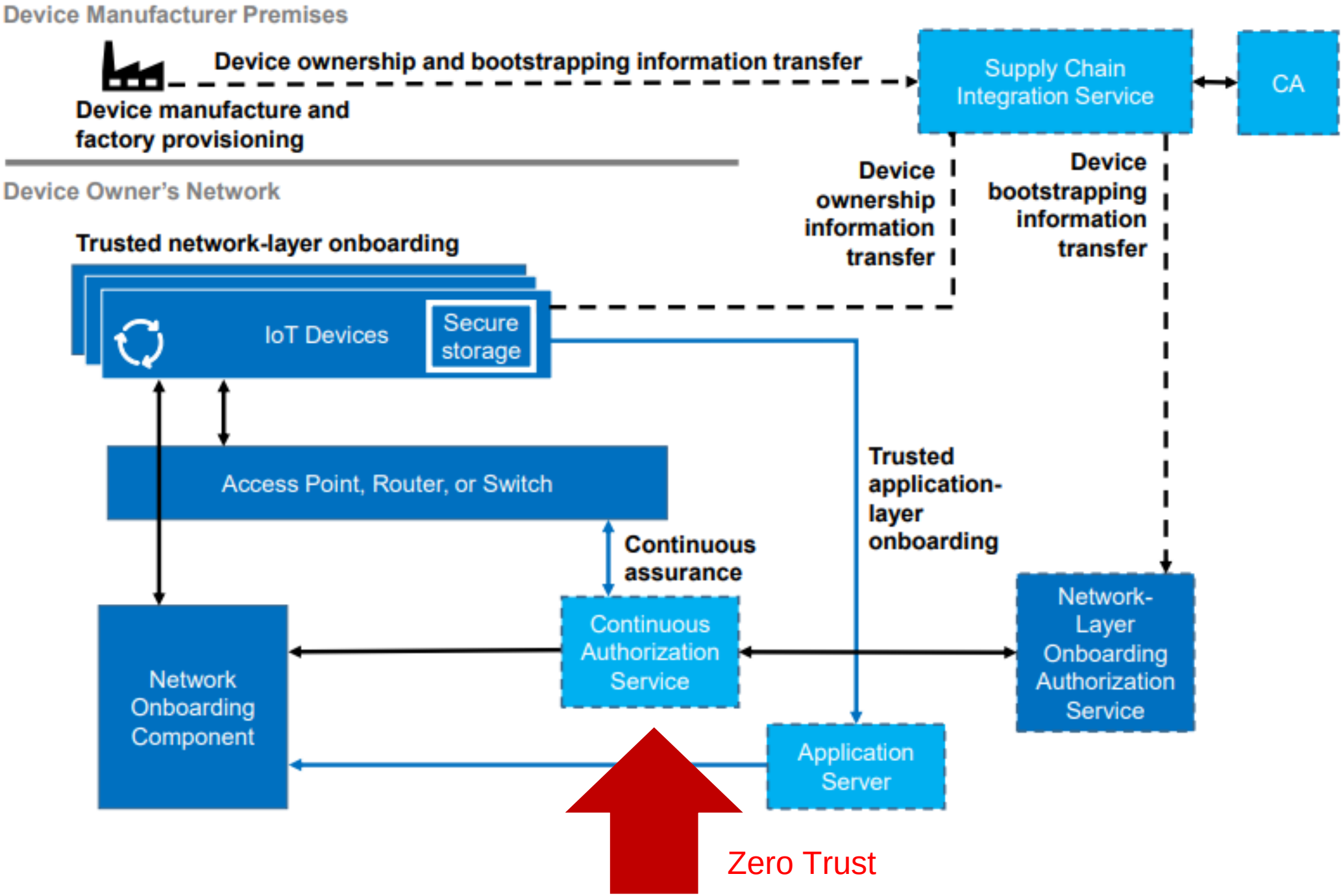
nquringminds

Trusted IOT Lifecycle

Big Picture – why is this important

- Usability
- Scalability
- Security improvements (continuous)
- Supply chain integration (business)


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


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

BRSKI Base

Build 5

IETF Standard

International standard under a royalty free regime

Generic

Solves the general problem of joining a security domain
Can be mapped to multiple physical network types

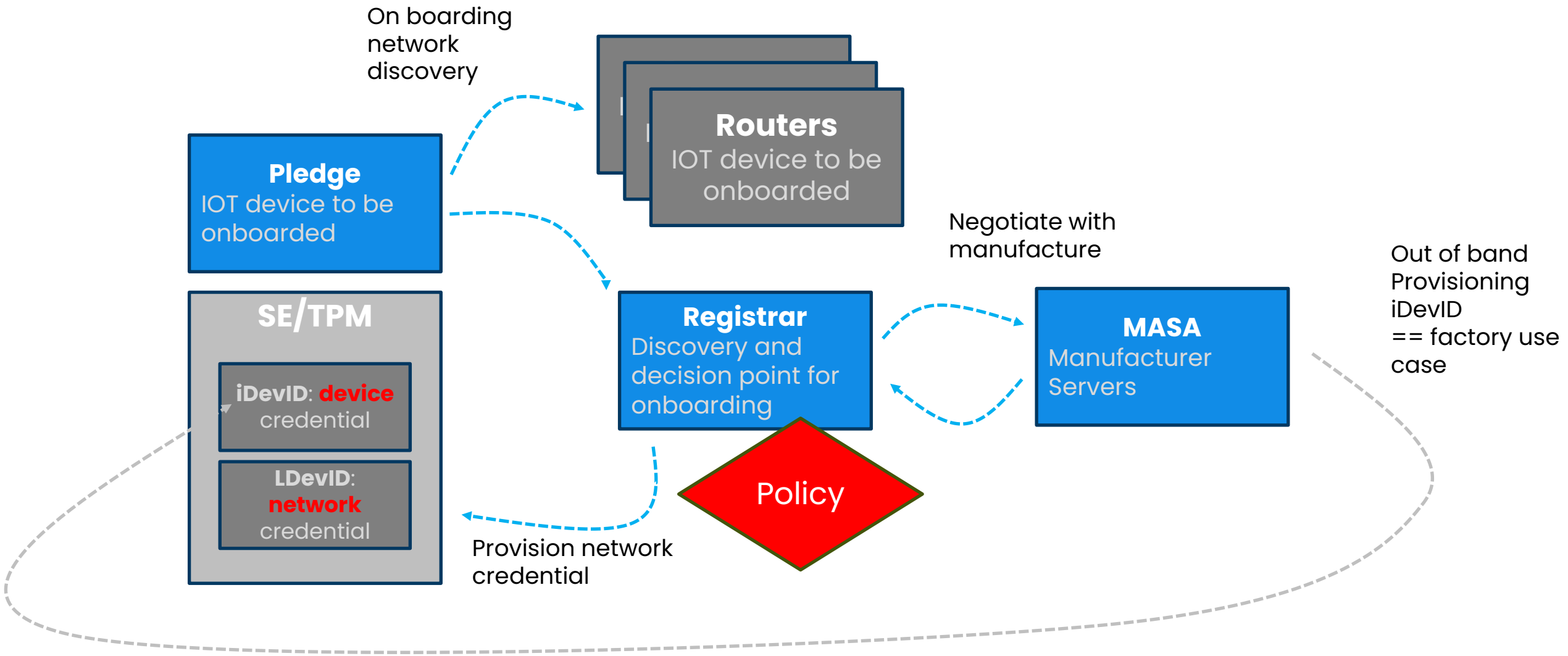
Supply chain

Models a full supply from device to network to manufacture

Strong security

Models a full supply from device to network to manufacture

BRKSK Flows


On boarding network discovery
Routers
IOT device to be onboarded
Pledge
IOT device to be onboarded
SE/TPM
iDevID: device credential
LDevID: network credential
Registrar
Discovery and decision point for onboarding
Policy
Negotiate with manufacture
MASA
Manufacturer Servers
Out of band Provisioning iDevID == factory use case
Provision network credential

Incremental Challenge…..

nquiringminds

Wi-Fi mapping

- Fully BRSKI mapping to Wi-Fi onboarding
- Specifically EAP-TLS certificate
- Unique onboarding certificate issued to each device
- Allows for per device revocation (lifecycle management)
- Lays ground work for more general management

Incremental Challenge.....

nquiringminds

Flexible Policy

- Build 5 support generalised and extensible policy
- Implements the decision points implicit in BRSKI
- Extends them and drives from a generic policy engine
- Policy evidence is presented interoperable through W3C Verifiable credentials

Policy

Policy implementation

nquiringminds

Policy	Description
Trusted Manufacturer	Checks the integrity and provenance of the iDevID (with the MASA)
Manufacture recognises device	An additional check where the manufacture checks against issued iDevIDs
Network owner trusts manufacturer	Network owner conditionally allows the Registrar talk to the manufactures website (MASA) (leakage)
Device instance trusted by network owner	The network owner specifically trusts this individual device , e.g enterprise onboarding process
Network owner trusts device type	Device type retrieved from MASA manged update server, is specifically trusted

Policy

Policy implementation

nquiringminds

Policy	Description
Trusted behaviour	MUD descriptor retrieved from “update server” is within parameter (optional allocation to subnet)
Trusted dynamic behaviour	Behaviour is continually checked against MUD file. Exception results in revocation
Trusted CVE level	SBOM retrieved from update server. Look-up CVEs and compare to threshold
Trusted CVE level dynamic	Registrar, continually checks against CVE databases, using SBOMS. If new critical CVE discovered - escalate

Learnings

Build 5

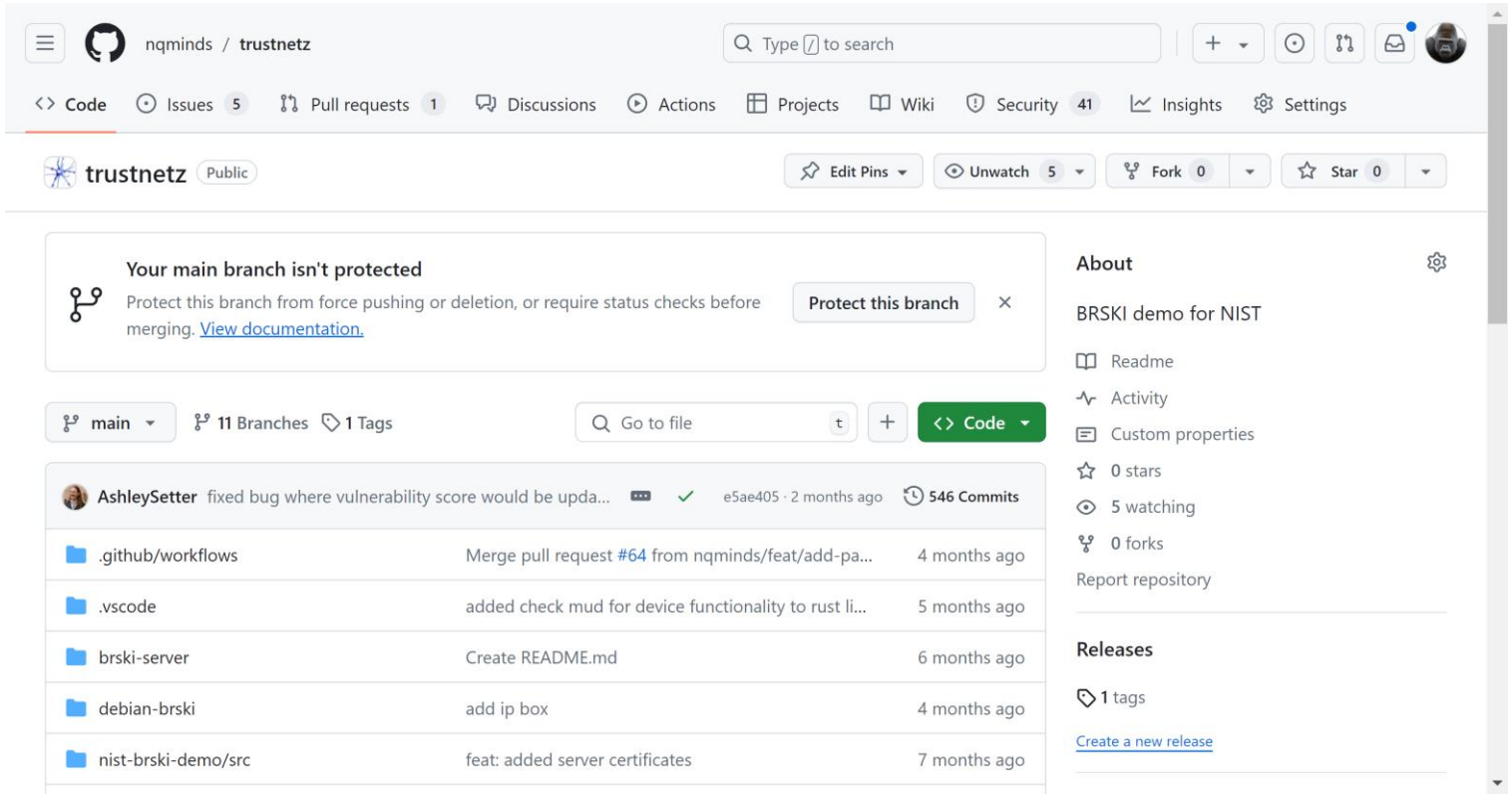
nquiringminds

Secure: EAP-TLS is a vast improvement, providing strong single device controls, but we need good protocols to provision.

DevID lifecycle: a single IDevID is fragile. We need more sophisticated identity lifecycle to manage SBOM and MUD at scale

Secure element: secure management of local credentials is critical. Code stacks need better support (e.g. EAP-TLS)

Flexible policy: expressing flexible policy with interoperable credentials, is invaluable to support different ecosystems and business modesl



Full implementation easily replicable on off the shelf Raspberry PIs

Generic code – easily adaptable to other platforms

All open sourced

Open source assets

https://trustnetz.org
https://github.com/nqminds/trustnetz

Questions

nick@nquiringminds.com
Nick Allott

NCCoE IoT Onboarding Project

Factory Provisioning Use-Case

Minerva.Sandelman.ca
Sandelman Software Works

SEALSQ
- Steve Clark
  - Security Technologist

Sandelman Software Works
- Michael Richardson
  - Chief Scientist

- July 10, 2024

The Factory Provisioning Use Case

- Objectives:
  - Demystify manufacturer provisioning
  - Simulate the pre-provisioned Secure Element scenario
  - Advocate that the identity of devices be provisioned by the manufacturer
  - Demonstrate online Certificate Management Service (CMS)
    - Using Trusted Certificate Authority (CA)
  - Document one or more flows involving BRSKI and DPP that uses a pre-provisioned secure element

SEAL SQ
semiconductors + quantum

Different Approaches to Provisioning

- Key-Pair Generated on IoT Device
- Key-Pair Generated in Secure Element
- Key-Pair Loaded into IoT Device
- **Key-Pair Pre-Provisioned onto Secure Element**
- Private Key Derived from Shared Seed

SEAL SQ
semiconductors + quantum

Typical Model of IoT Device Production – without Secure Element

- Device Board is Assembled
- Board is connected to “Bed of Nails” for setup and provisioning
- Diagnostic firmware is loaded
- Basic functionality is tested
- Keys and Certificates are loaded
  - This step requires a secure facility
- Production firmware is loaded
- Final test of IoT device

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

SEAL SQ
semiconductors + quantum

Typical Model of IoT Device Production – with Pre-Provisioned SE

- Device Board is Assembled
  - SE protects keys and certificates – secure facility requirement is minimized
- Board is connected to “Bed of Nails” for setup and provisioning
- Diagnostic firmware is loaded
- Basic functionality is tested
- Production firmware is loaded
- Final test of IoT device

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

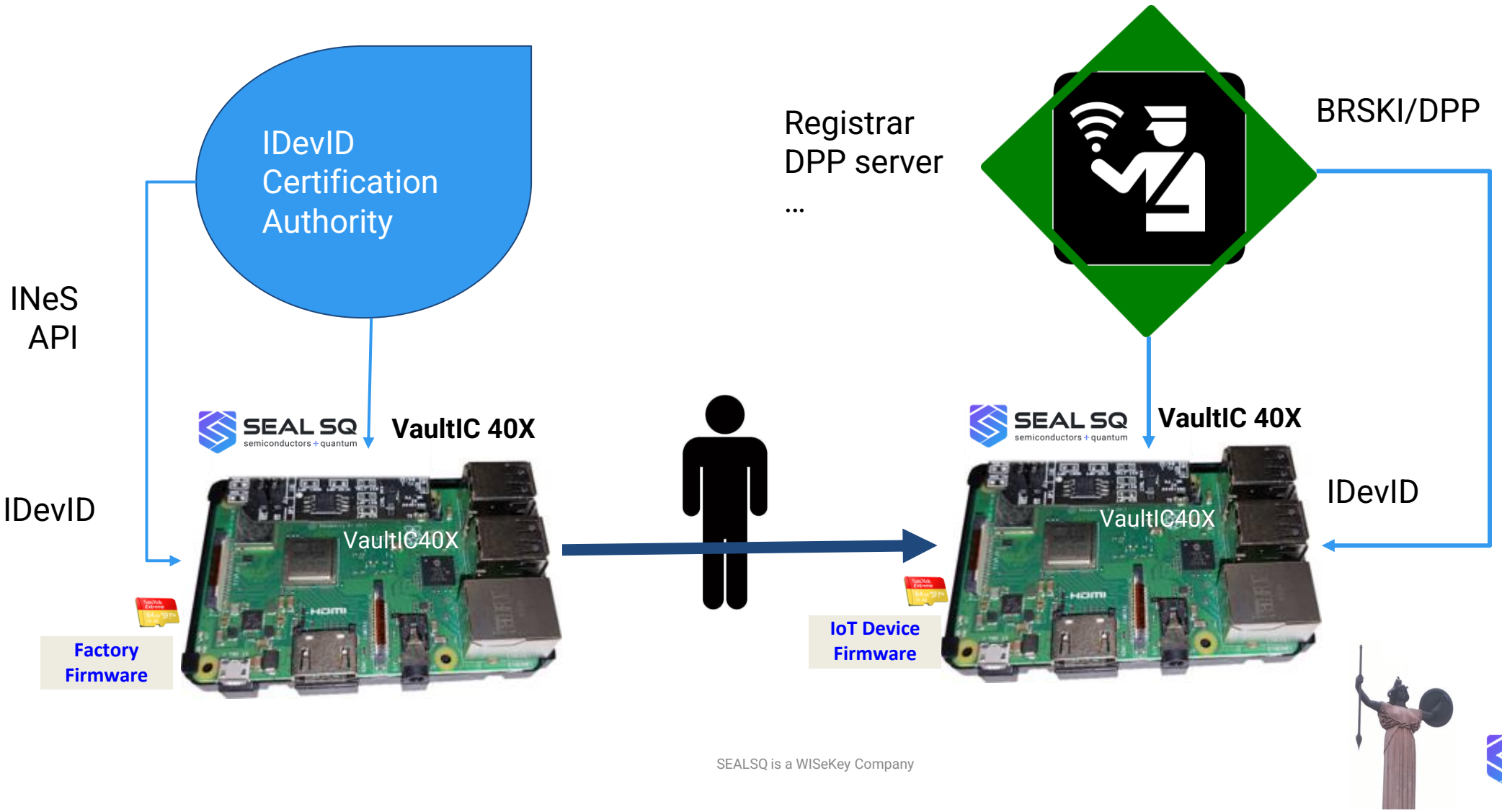
SEAL SQ
semiconductors + quantum

The Demo

- Limitations
  - Key provisioning and firmware loading process for RPI involves manipulating SD cards
- Implementation
  - Pre-provision a secure element with an immutable Identity
    - Key-Pair / Certificate
  - Install the secure element on an IoT edge device to establish the platform hardware root of trust and Identity
- Technologies
  - Raspberry Pi Platform
  - VaultIC40X Secure Element from SealSQ
  - INeS Certificate Management System API
  - INeS-Hosted Certificate Authority

SEAL SQ
semiconductors + quantum

Overview Factory Provisioning Use-Case Demo



SEAL SQ
semiconductors + quantum

Q & A

THANK YOU

SEAL SQ
semiconductors

Build 1: Enterprise IoT Onboarding

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Dan Harkins
Danny Jump

HPE aruba networking

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, establishment of a secure connection
  - 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)

Build 1: 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*
- Device is automatically discovered, recognized, and onboarded

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

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
- Remote office employee just unpacks, plugs device in, it is automatically provisioned

Benefits of DPP

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

Simple, secure, robust onboarding workflow

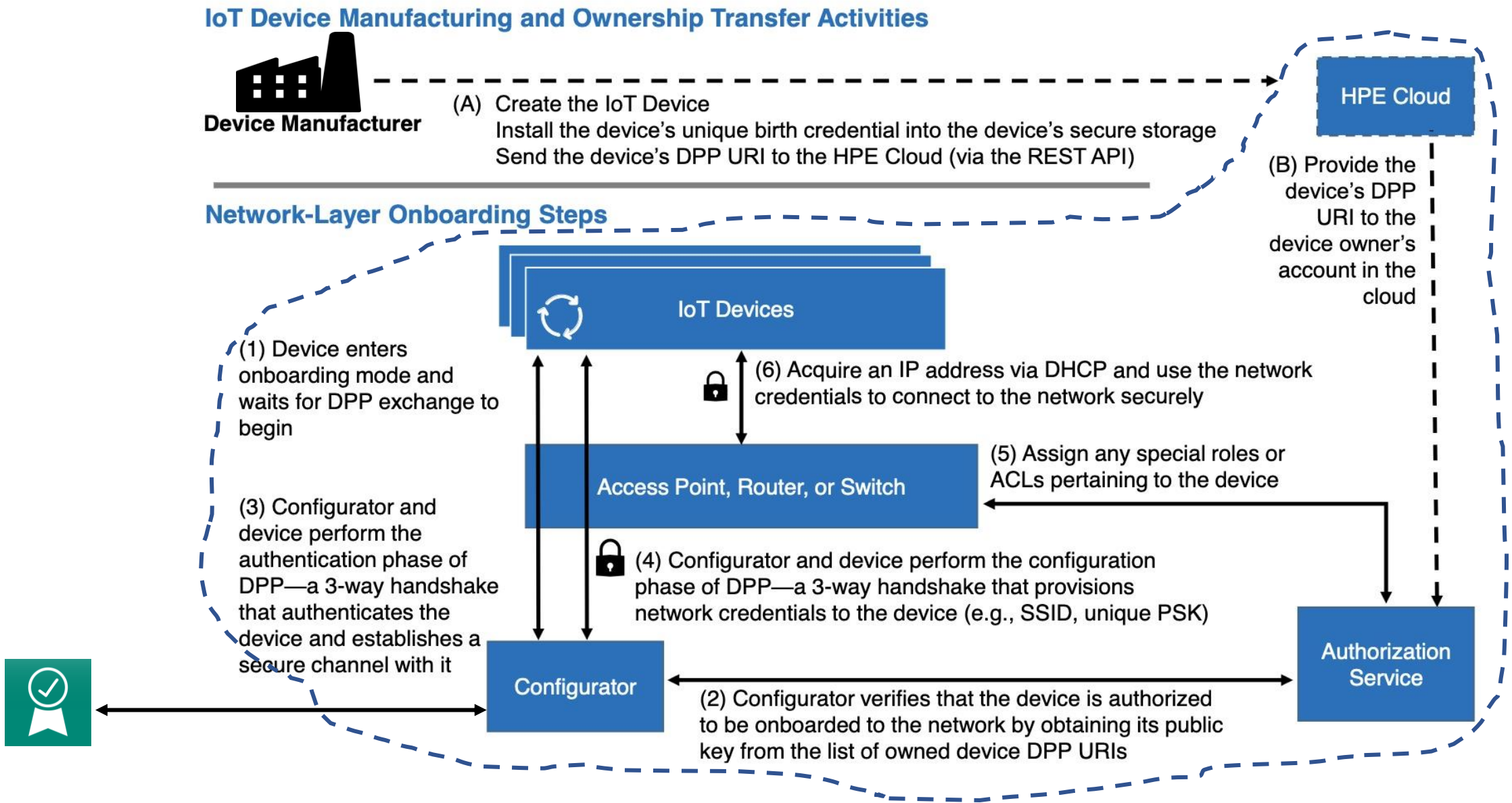
No rigid onboarding process to follow– bootstrapping can take place before or after device is installed

Onboarding at scale

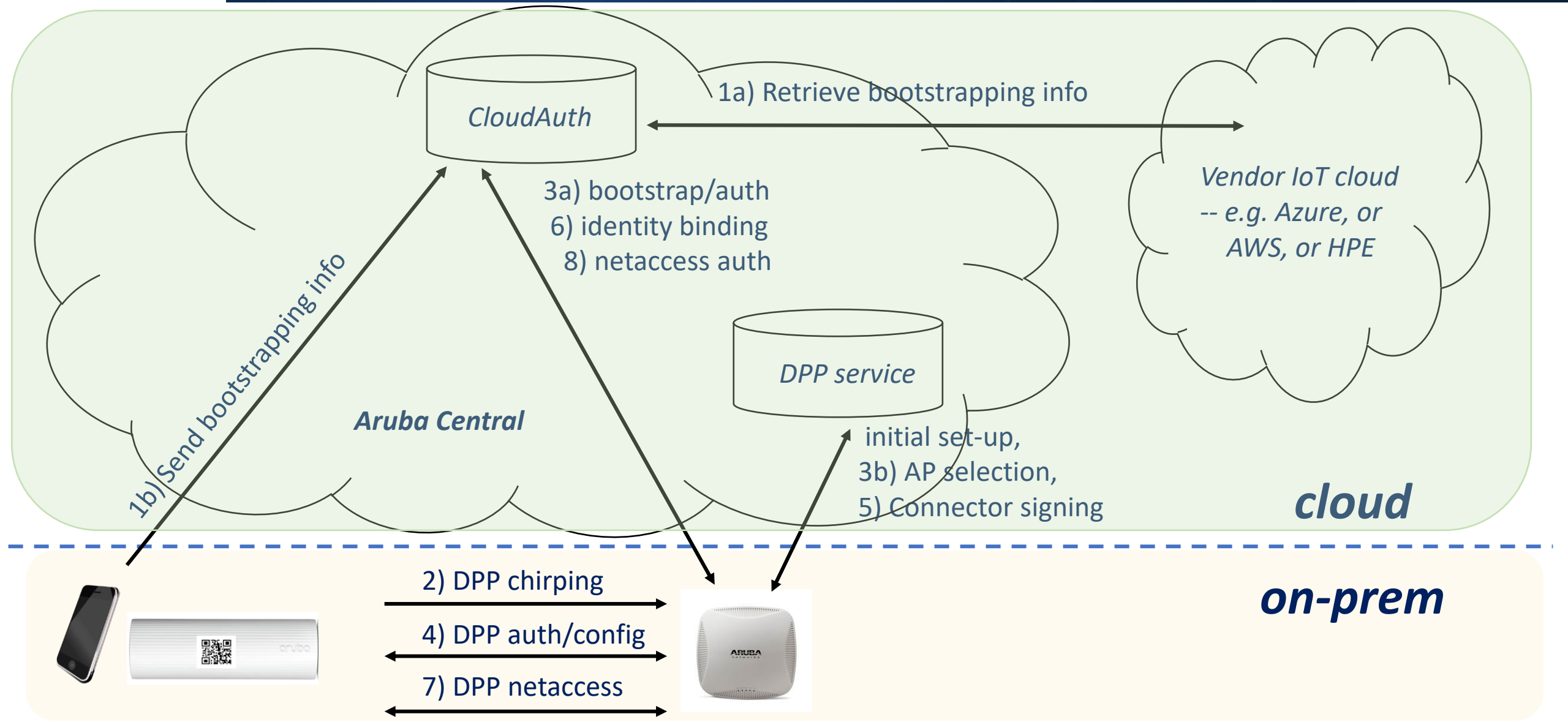
Zero touch onboarding

Can provision all credentials used in modern 802.11 networks

Build 1 and the Notional Architecture



Build 1's DPP Architecture– DPP As A Service



Build 1 Capabilities

Current

Trusted Network-layer Onboarding

- Device discovery, 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

→ Integration with public, trusted CA for certificate issuance

→ Factory-generated keypair on TPM, automatically generated DPP URI and QR code

Planned

MUD (RFC 8520) integration

Thank You!


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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE


HPE aruba
networking

CableLabs

Build 2

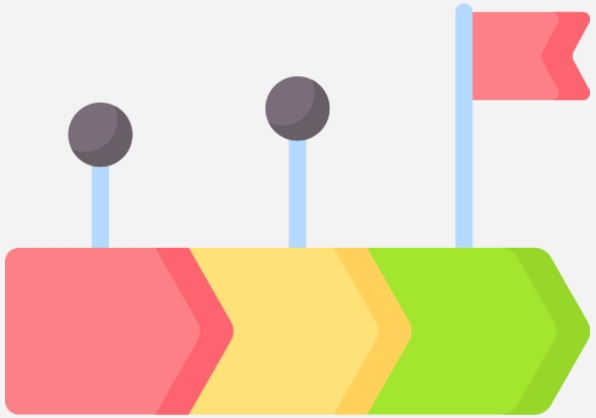
WI-FI EASY CONNECT, CABLELABS, OCF

Andy Dolan, Senior Security Engineer
Craig Pratt, Lead Software Engineer

WI-FI NETWORK ONBOARDING: GOALS

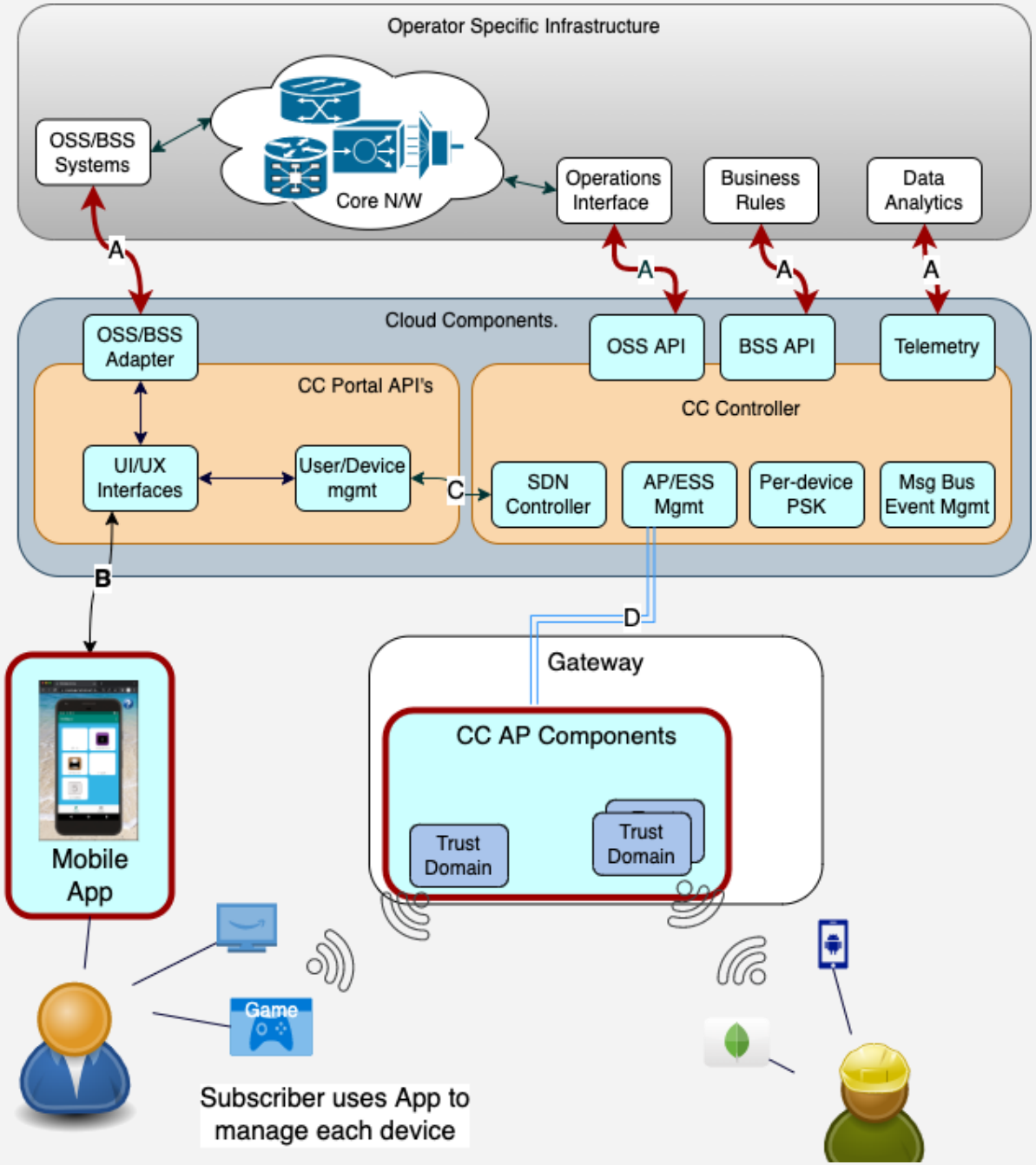
Demonstrate:

- Secure network (L2/L3) onboarding
  - Using DPP/EasyConnect (WFA) and Custom Connectivity (NetReach; CableLabs) 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



CUSTOM CONNECTIVITY ARCHITECTURE

- **Network Onboarding Component:**
  - DPP/EasyConnect (WFA)
  - Custom Connectivity/NetReach (CableLabs)
- **Authorization Service:**
  - The Custom Connectivity 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



Custom Connectivity onboarding enables devices to be given *unique* credentials. Each device has a unique *identity* and *policy* that follows the device

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

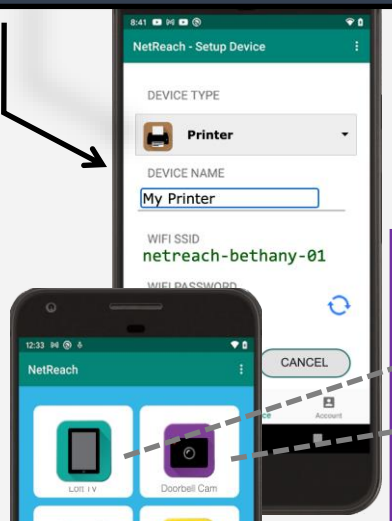
Once onboarded, device policy can be modified and credentials can be revoked without affecting other devices in the household

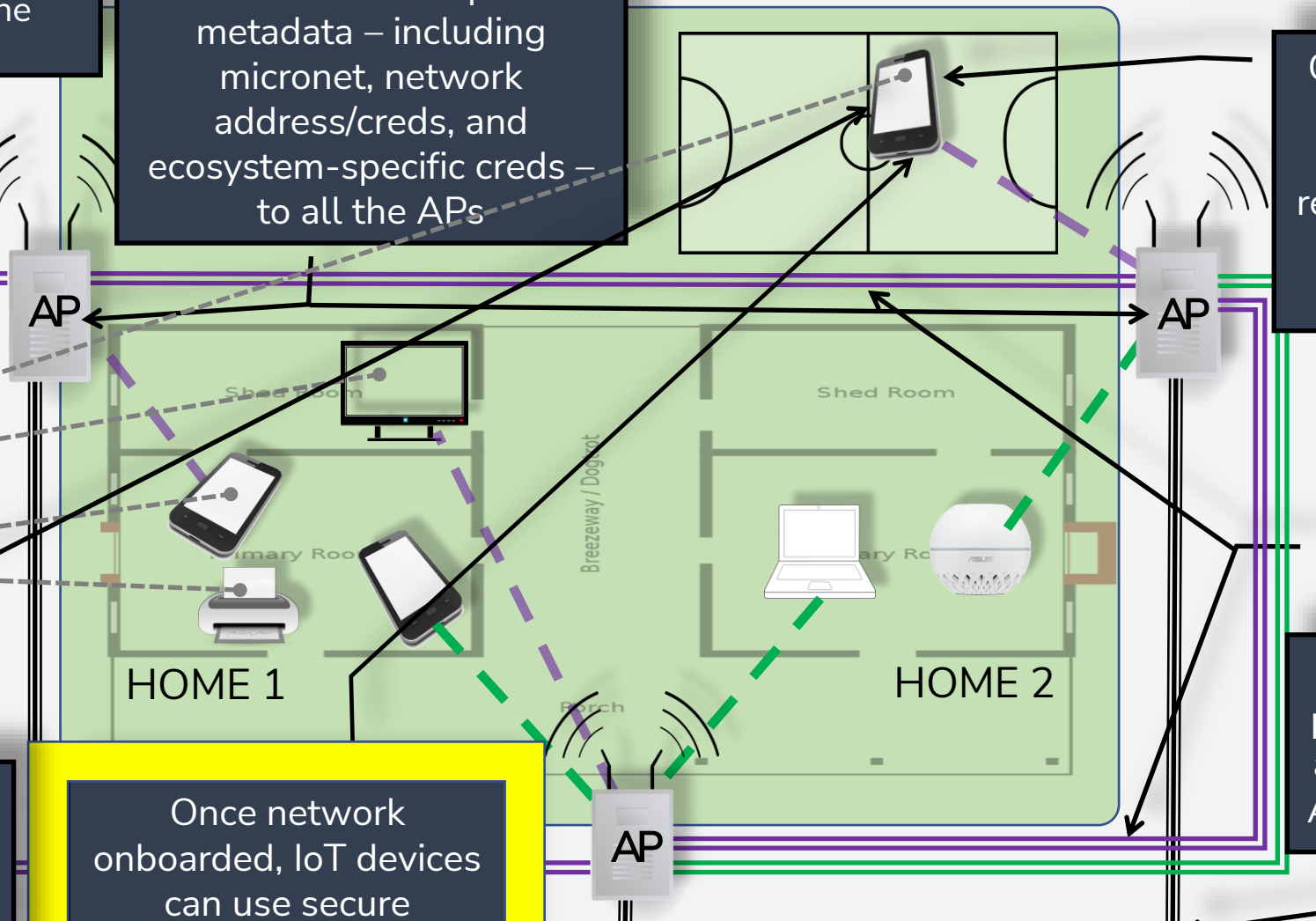
APs establish vxlan tunnels with peers APs on-demand over shared backhaul

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 Custom Connectivity and switch APs if/when necessary

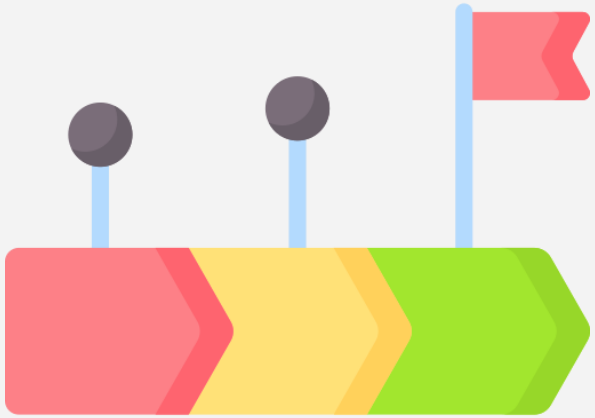
Once network onboarded, IoT devices can use secure onboarding metadata to start L4 onboarding



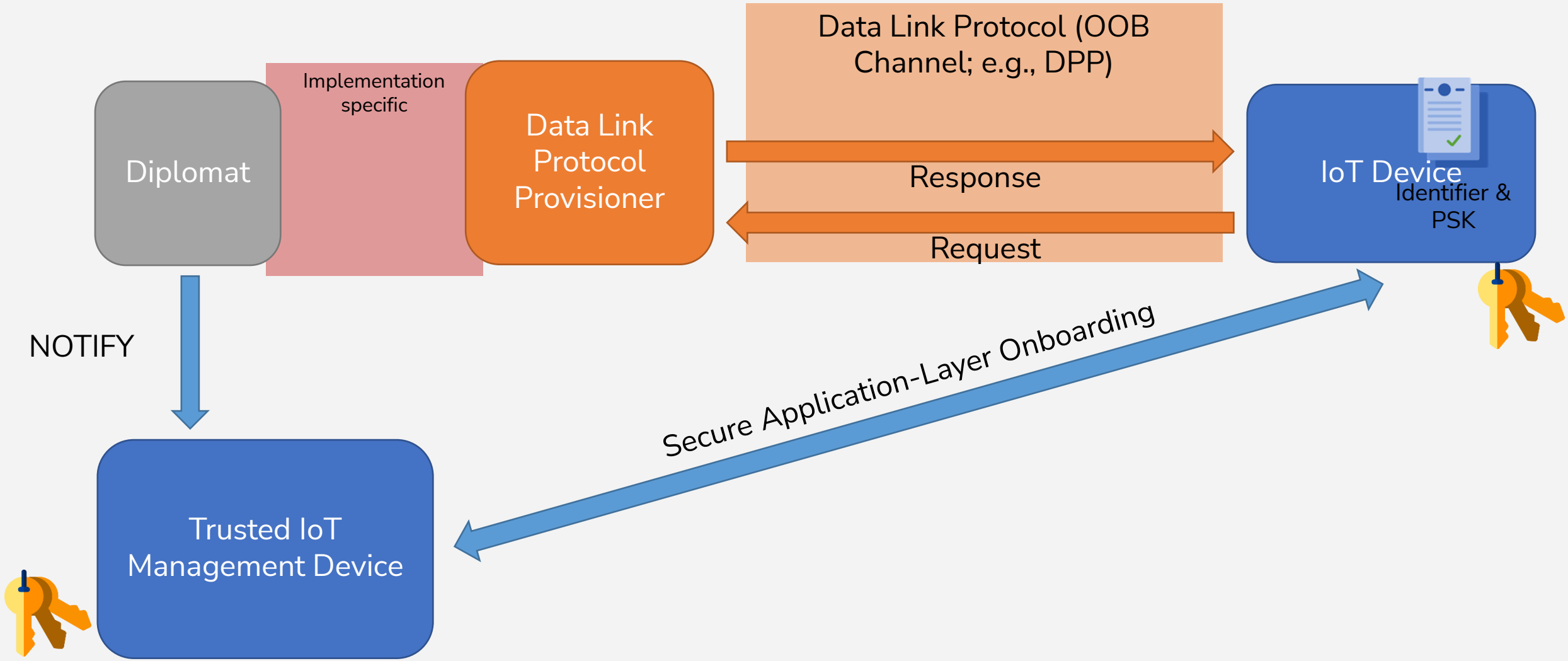


STREAMLINED ONBOARDING: GOALS

- 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



STREAMLINED ONBOARDING OVERVIEW



CableLabs®

Build 2

THANK YOU

Audience Q & A

Please submit questions to our panelists using the Zoom Q&A feature.

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

Comment period open until **July 30, 2024**

nccoe.nist.gov

@NISTcyber

iot-onboarding@nist.gov