

A summary of the NIST NCCoE Trusted IoT  
Device Network-Layer Onboarding and  
Lifecycle Management effort  
2024-10-30, RIPE89, IETF121 T2TRG

<https://www.sandelman.ca/SSW/talk/2024-ssw-nccoe-iot>

Michael Richardson <[mcr+ietf@sandelman.ca](mailto:mcr+ietf@sandelman.ca)>

# What is NIST/NCCoE?

- NIST = National Institute of Science and Technology
  - many many things
  - AES!
- “To promote U.S. innovation and industrial competitiveness by advancing measurement science , standards , and technology in ways that enhance economic security and improve our quality of life”
- National Cybersecurity Center of Excellence  
[nccoe.nist.gov](http://nccoe.nist.gov)
- “Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs.”
  - Collaboration with Industry, Federal/State/Local Governments, and Academia
- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

## Project Abstract

Provisioning network credentials to IoT devices in an untrusted manner leaves networks vulnerable to having **unauthorized** IoT devices connect to them. It also leaves IoT devices vulnerable to being taken over by **unauthorized** networks. Instead, trusted, scalable, and automatic mechanisms are needed to safely manage IoT devices throughout their lifecycles, beginning with secure ways to provision devices with their network credentials—a process known as **trusted network-layer onboarding**. Trusted network-layer onboarding, in combination with additional device security capabilities such as device attestation, application-layer onboarding, secure lifecycle management, and device intent enforcement could improve the security of networks and IoT devices.

NIST SP 1800-36 (Complete draft guide)

NIST SP 1800-36A: Executive Summary (Draft)

NIST SP 1800-36B: Approach, Architecture, and Security Characteristics (Draft)

NIST SP 1800-36C: How-to Guides (Draft)

NIST SP 1800-36D: Functional Demonstrations (Draft)

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

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

## Project Timeline

- 1) 2020-ish, rumours about the effort
- 2) 2021 – Federal Registry Notice released giving formal notice
- 3) June 2022 – Project launch, engineering day to install lab
- 4) 2022/2023 – Twice Monthly collaborator calls
- 5) work on various project briefings
- 6) 2023 – Build 5 and build 6 deployed
- 7) 2024 – project wrapping up
- 8) Winter 2025 – engineer day wrap up



## Build 1: Wi-Fi Easy Connect Protocol (DPP), Aruba/HPE

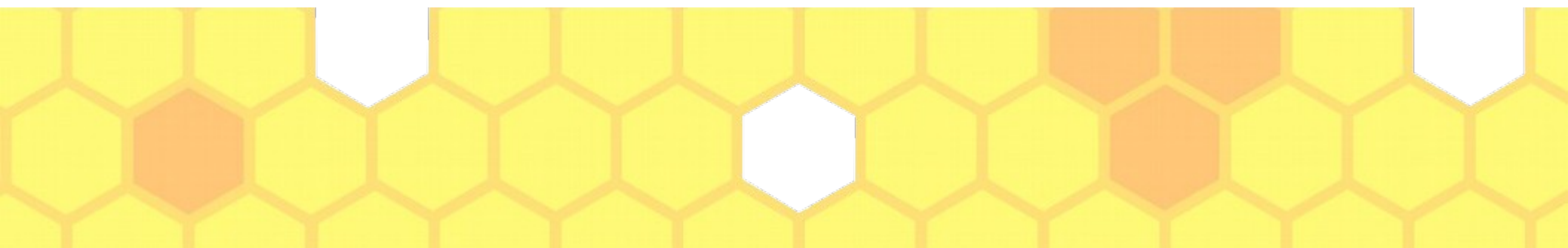
- Independent Application-Layer Onboarding to UXI Cloud

Collaborators: Aruba, an HPE Company (Build Champion), CableLabs, NXP Semiconductors, SEALSQ, a subsidiary of WISEKey


## Build 2: Wi-Fi Easy Connect Protocol (DPP), 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:RFC8995) Protocol, Sandelman Software Works

Collaborators: Sandelman Software Works (Build Champion), 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:RFC8995) Protocol, NquiringMinds

Collaborators: NquiringMinds (Build Champion), Sandelman Software Works, SEALSQ, a subsidiary of WISEKey





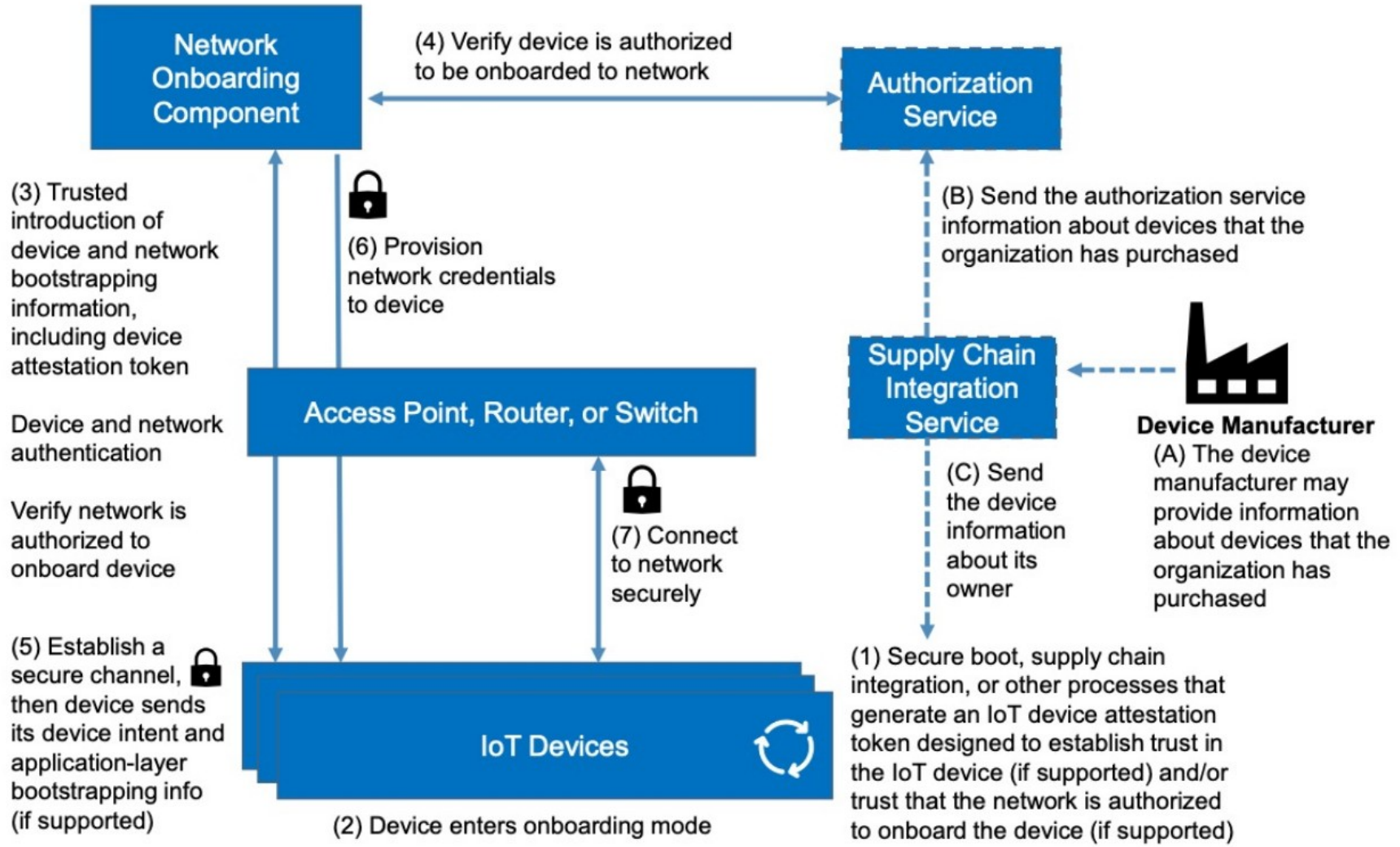
# Factory Provisioning Use-Case (cross-build application)

Collaborators: Aruba, an HPE Company, Sandelman Software Works, SEALSQ, a subsidiary of WISEKeyWhat's Nex

This case (notionally build6) is actually applicable to all other cases, and a prerequisite. This is about device id (802.1AR) provisioning.

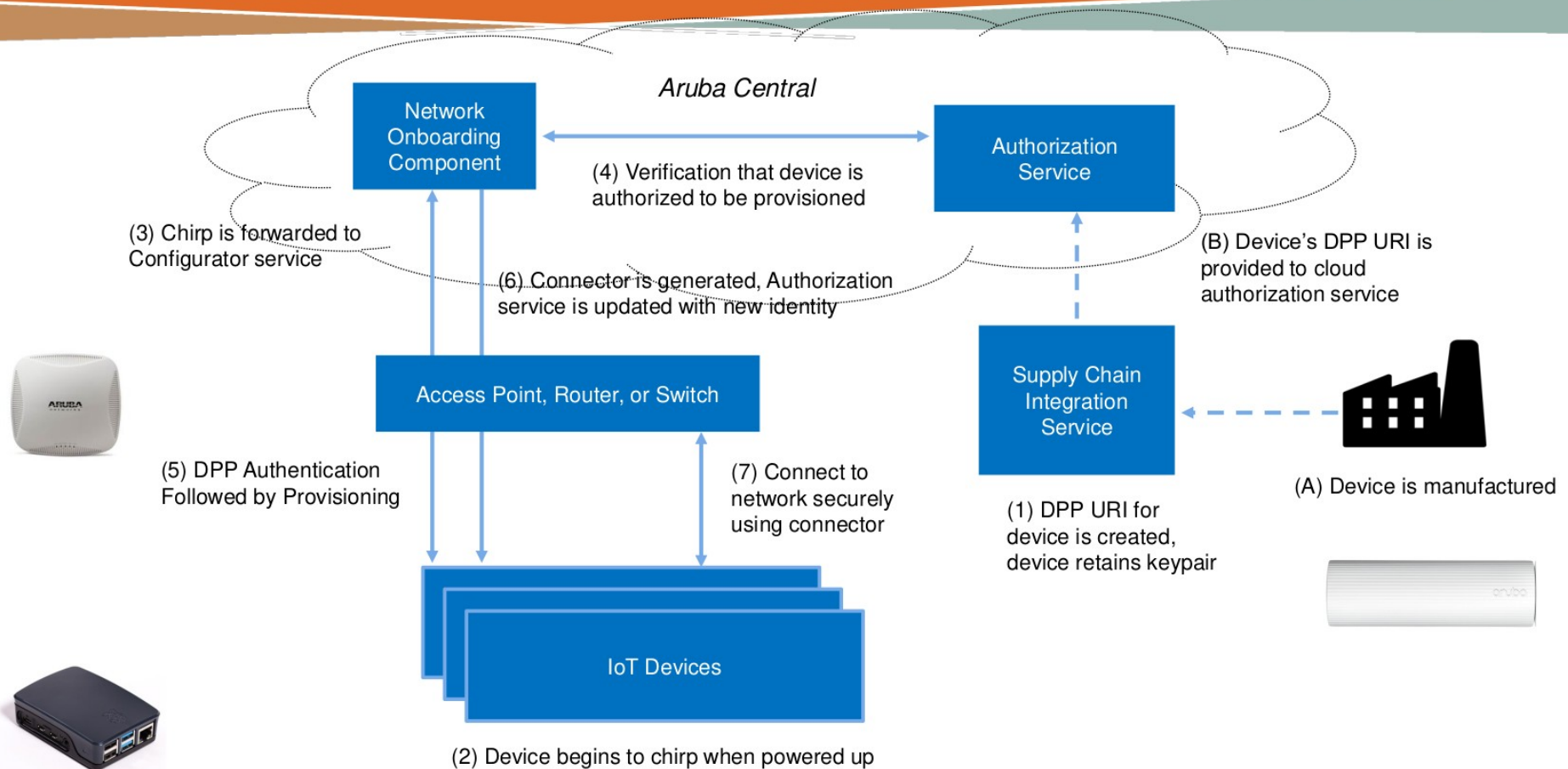


# High Level Architecture

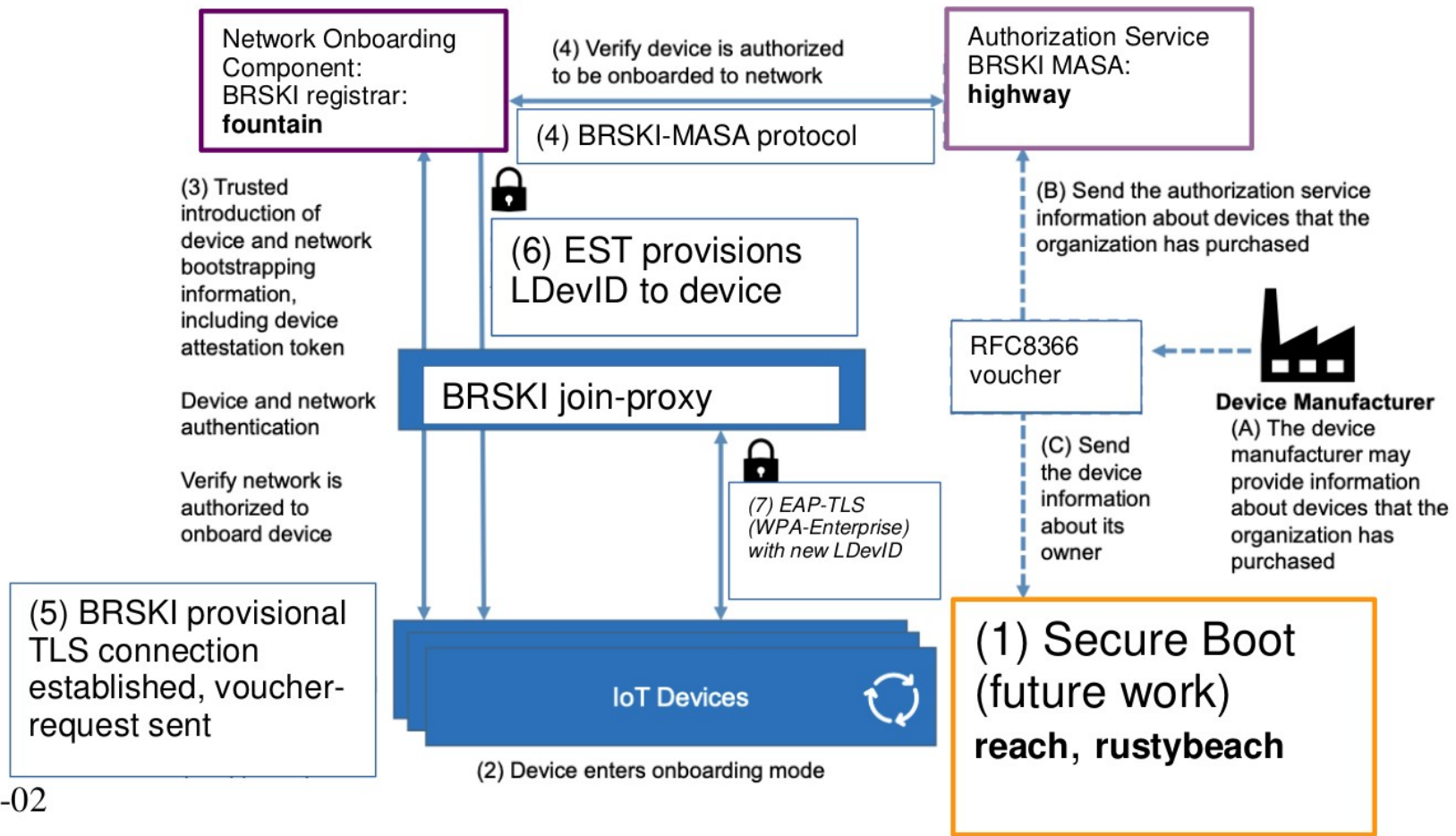




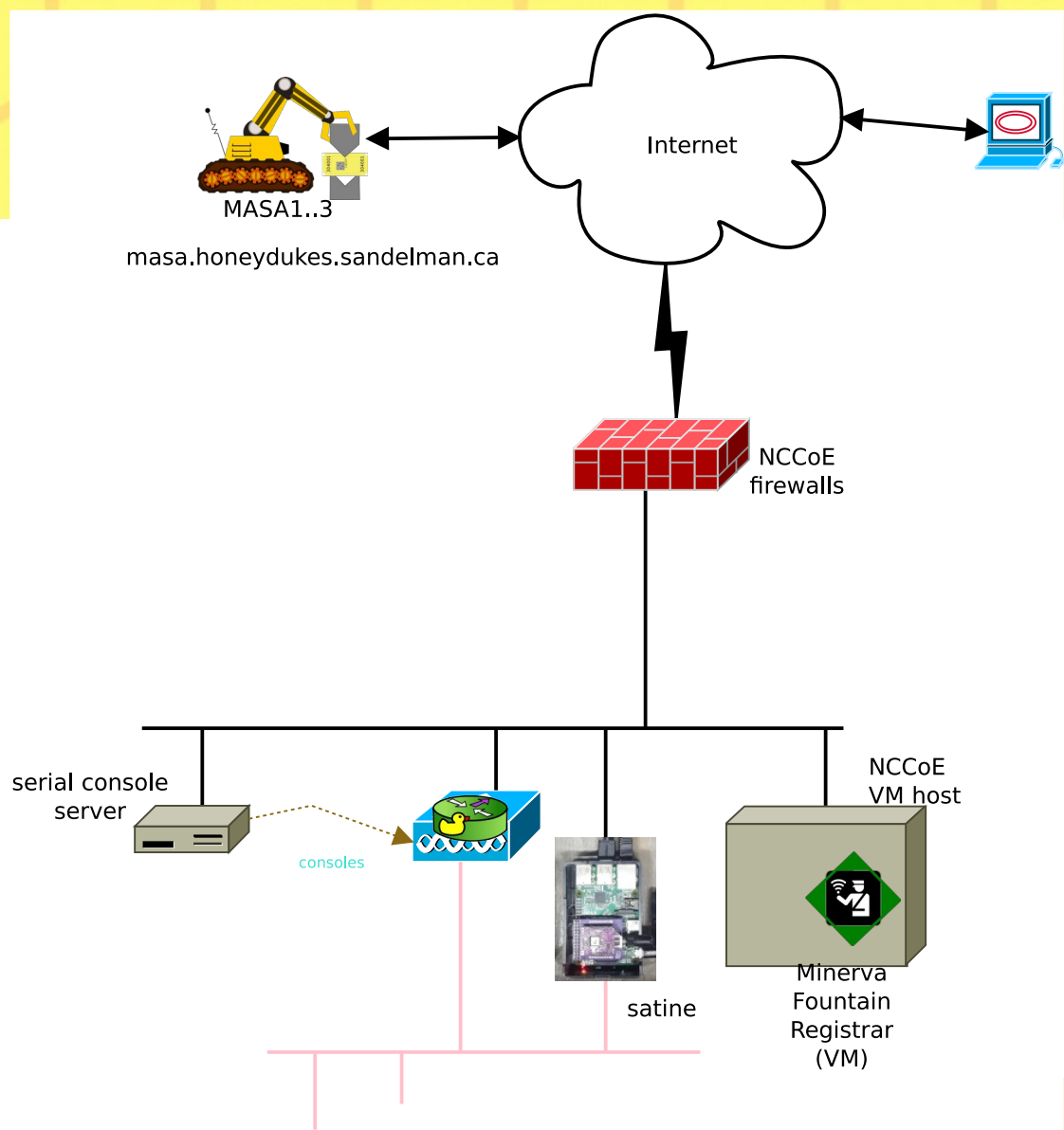
# DPP and the IoT Onboarding Notional Architecture



# Project components available



2022-06-02



[brski.org](http://brski.org)



Uplink cable

DMZ Switch

nRF52840:  
802.15 onboarding

esp32-wifi  
onboarding

satine: machine  
behind switch,  
LAN onboarding  
802.15.4 gateway

nrf52840  
console server

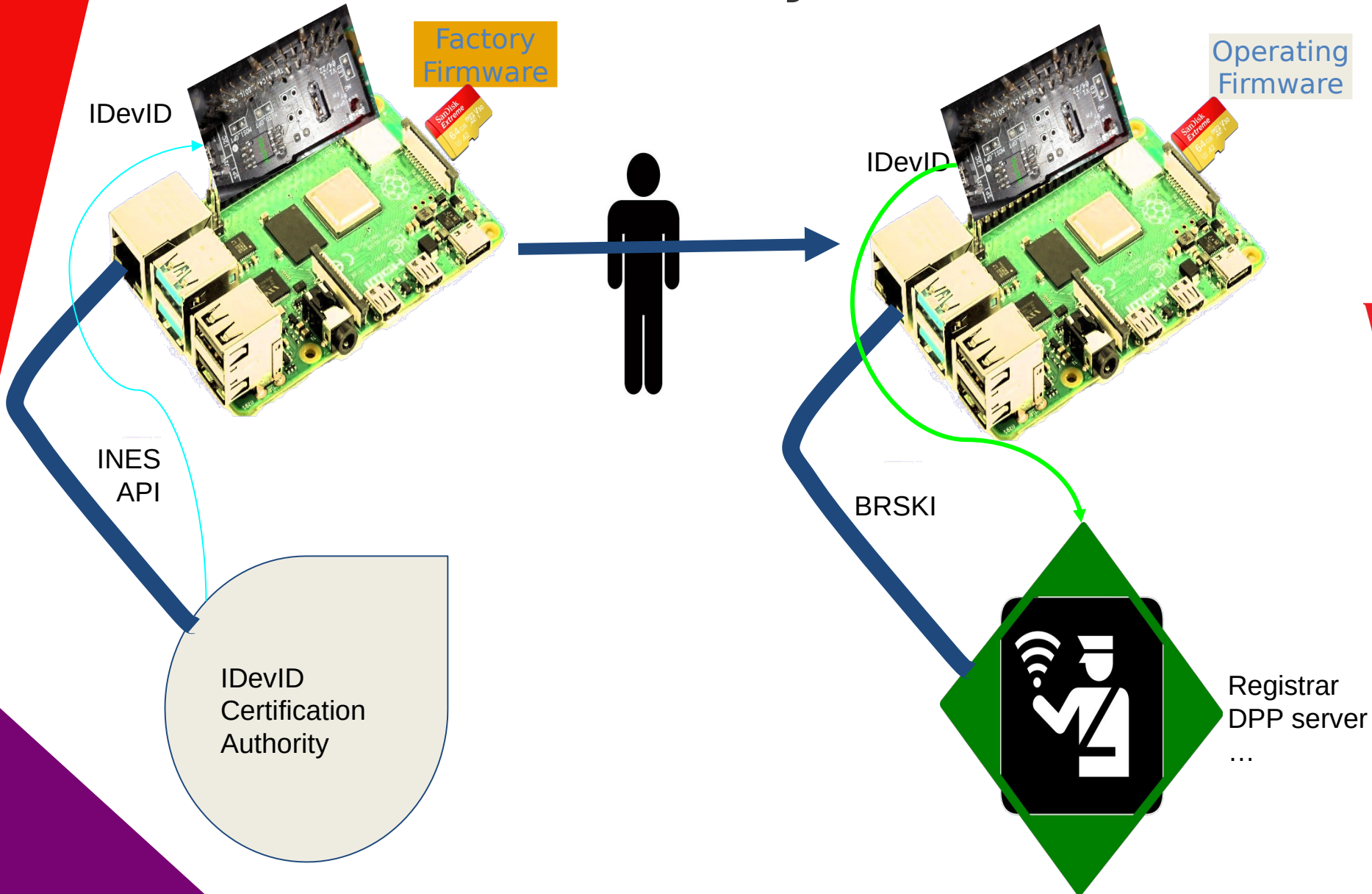
Onboarding Router

5v USB power  
amb-s-usb

Vertiv



# Overview Factory build6 demo



WIS@key



QUESTIONS/DISCUSSION

