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

Deployment Challenges with IoT

- On-boarding Catch-22
  - Need to get on the network to get a credential
  - Need a credential to get on the network
- Many *things* lack a functional user interface
- Deployment requires an insecure leap-of-faith
  - Small window of time at which device is susceptible to attack
  - Pass sensitive security credential in the clear
- Provisioning requires multiple, time-consuming steps per device
  - Boot-up as “soft AP”, advertise fixed SSID
  - Configure local IP address/default route on computer
  - Configure credential on device via web browser on computer (leap-of-faith)
  - Reboot device as client, use credential to access network
- Whole process is insecure, O(n) scale, requires expertise on location

HPE aruba networking

Deployment Challenges for Enterprise IoT

- Enterprise networks typically involve thousands of devices and scores of APs, compounding existing onboarding difficulties
- Proprietary techniques for onboarding causes problems
  - Sequential, one-by-one processing does not scale
  - Education on each device’s unique caveats for onboarding is unreasonable
  - IT expertise expected
- Not an Internet of *things*, a large network with *things*
  - Per-device credentials– no shared PSKs for every*thing*
  - Centralized policy enforcement for *things*
  - Continuous monitoring of *things*
  - Isolation of *things* on network
- Some *things* are mobile, security and policy have to follow

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, optional strong authentication of network by device, establishment of a secure connection

Provisioning– configuring network credentials in device

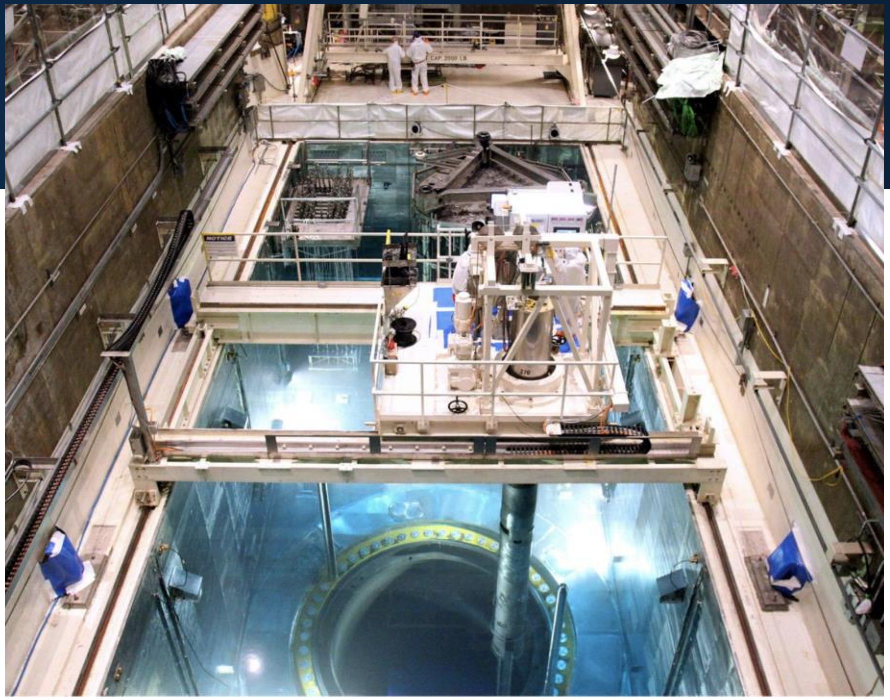
Network Access– secure connection to network to enable application-layer onboarding

Uses 802.11 action frames (pre-association, no SSID, no soft-AP)

DPP Features

- 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
  - Bootstrapping of trust in *thing*
  - Authentication of *thing* to network (optionally network to *thing*)
  - Provisioning of credential and network profile on *thing*
  - *thing* connects to network
- No rigid process to follow– bootstrapping can take place before or after device is installed
- Workflow is, “plug it in, turn it on…you’re done”
- Can provision all 802.11 credentials– DPP adapts to the network, not the other way around

Benefits of Enterprise DPP



Deployment at enterprise scale

- Devices are bootstrapped en masse
- Once bootstrapped, provisioning is automatic
- No longer an O(N) operation

Simplified deployment– turn it on, walk away

- No special IT expertise needed
- No laborious process involved

Drop ship deployments

- New equipment is automatically provisioned
- Centralized enforcement of policy on remote sites

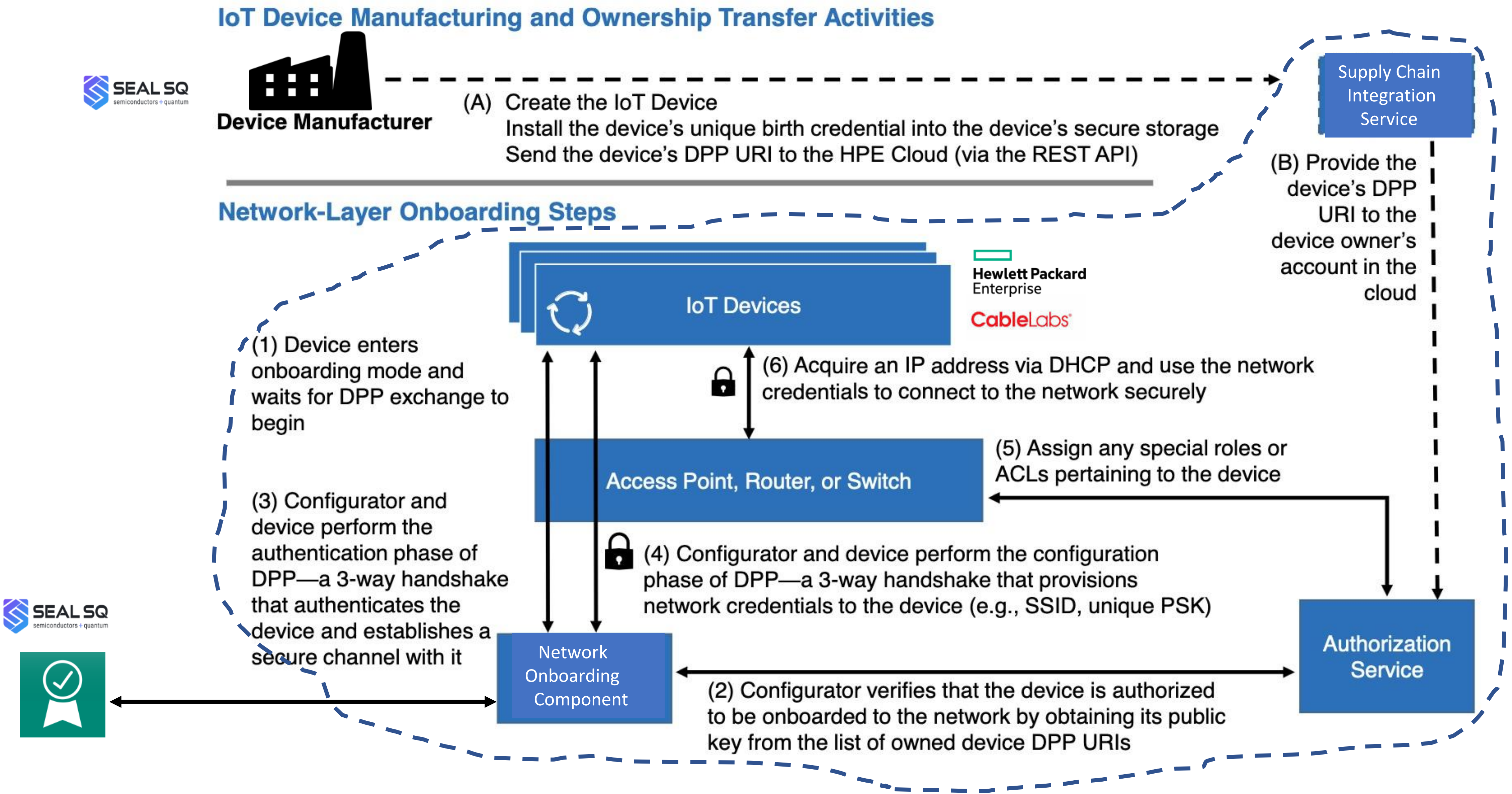
Dangerous, difficult deployments

- Nuclear power plant, offshore oil rig
- Worker just mounts and powers on device

Build 1: Onboarding for Enterprise

- Bootstrapping credential (DPP URI) created at manufacturing time
- Transfer of ownership of *thing*
  - Purchase order transfers DPP URI from vendor cloud
  - Published open REST API framework for generating custom onboarding applications
  - 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, authenticated, and onboarded
- DPP supports the all credentials used by the network
- No IoT or networking expertise needed to onboard things

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)

Supply Chain Integration Service

(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

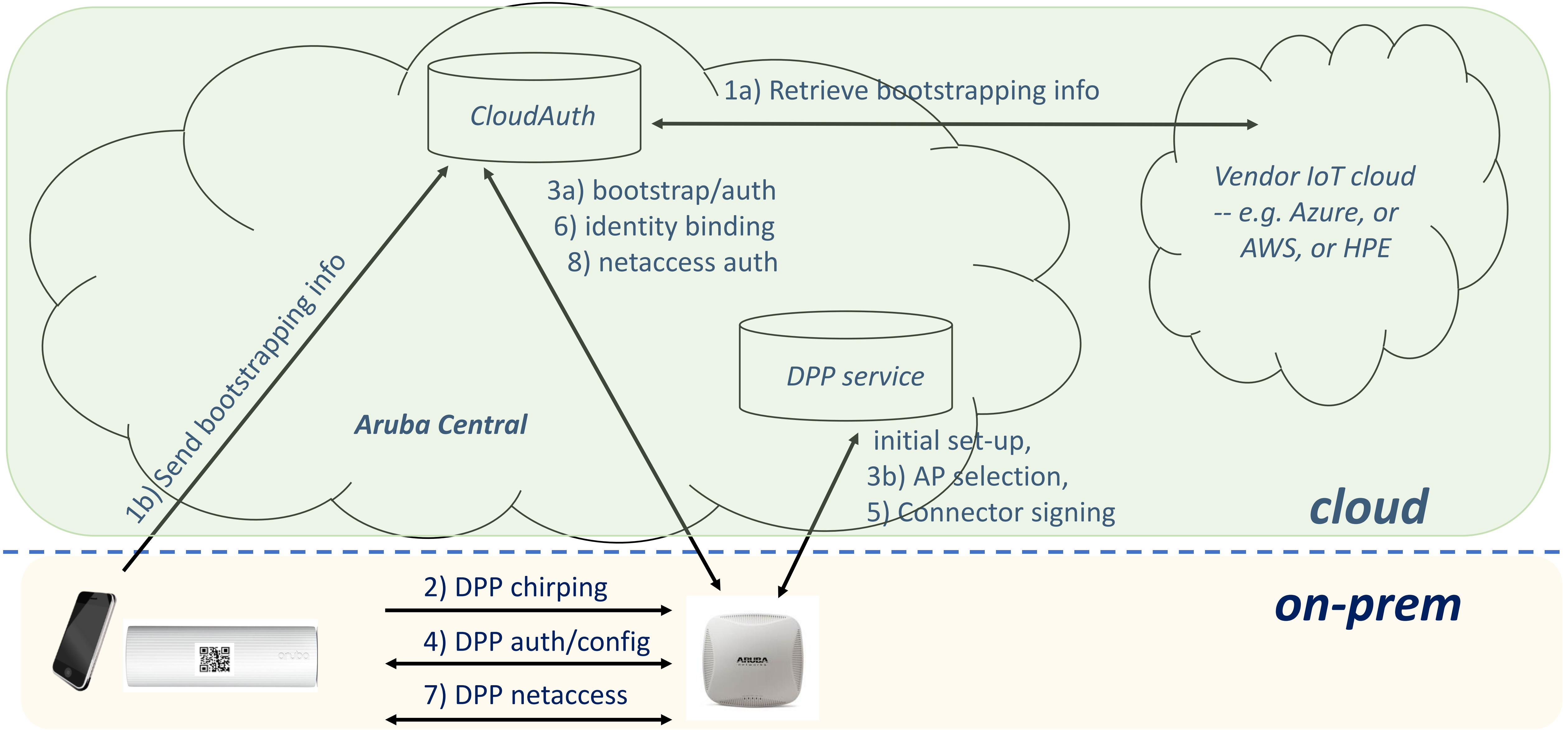
(4) Configurator and device perform the configuration phase of DPP—a 3-way handshake that provisions network credentials to the device (e.g., SSID, unique PSK)

Network Onboarding Component

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



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
- Centralized policy enforcement of *things* on the network

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

* Using DPP reference implementation on Raspberry PI

Thank You!

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

HPE aruba networking