

NCCoE Emergency Procedures

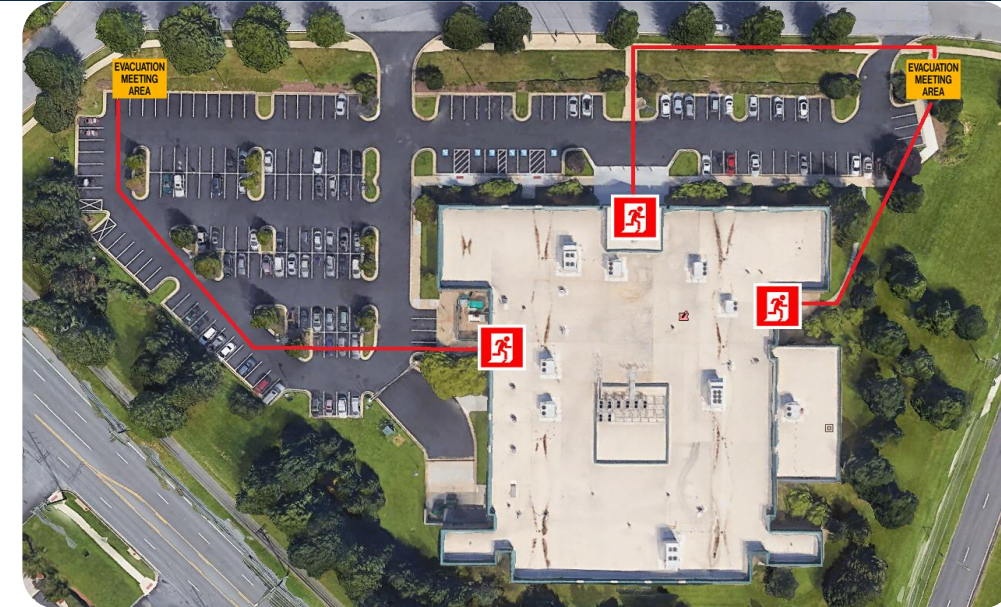
Evacuation Emergencies

What is an Evacuation Emergency?

- Fires
- Explosions
- Earthquakes
- Indoor toxic material releases
- Indoor radiological and biological accidents
- Workplace violence

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest exit (**Red Signs** – Upper Right Map)
- If the Security Guard is close by and accessible, ask for further instruction
- Once outside the building, swiftly walk toward the designated meeting area. (**Yellow Signs** – Upper Right Map)



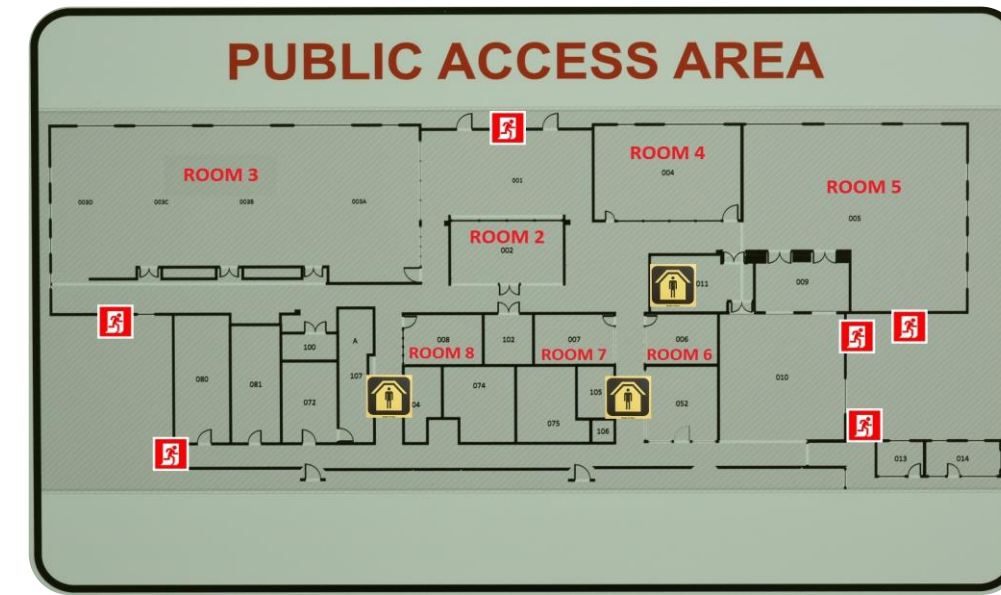
Shelter-In-Place (SIP) Emergencies

What is a Shelter-In-Place Emergency?

- Severe weather (hurricanes, tornadoes, etc.)
- chemical, biological, or radiological contaminants released into the environment

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest SIP hallway or room (**Yellow Signs** – Lower Right Map)
- If the Security Guard is close by and accessible, ask for further instruction



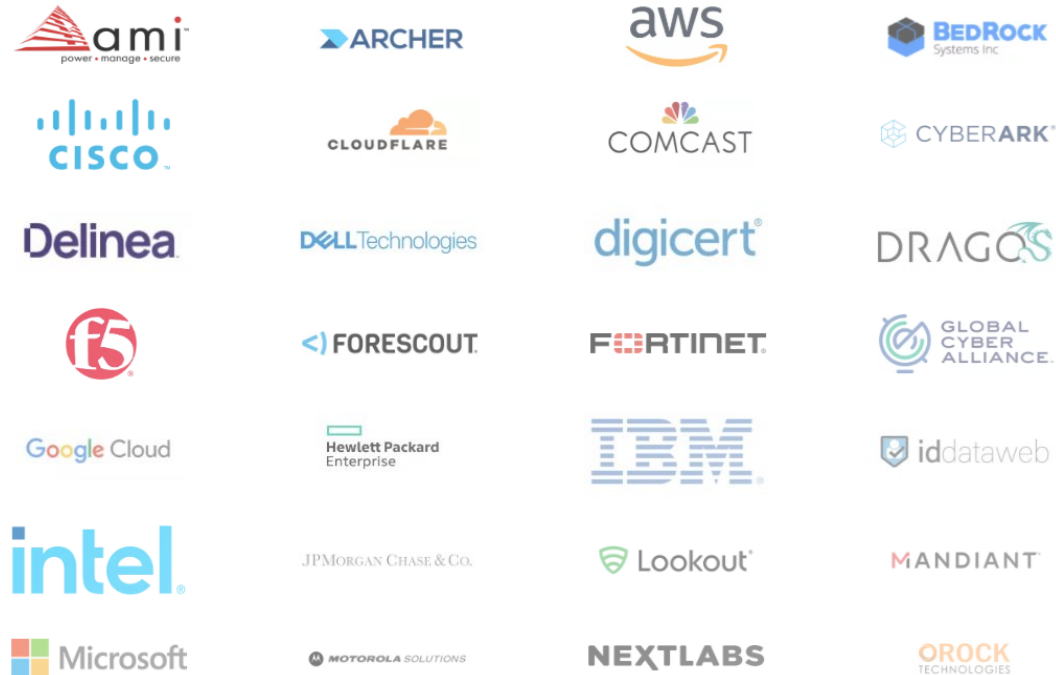


NIST-Guest

Open Wi-Fi

Connect your device to the "NIST-Guest" Wi-Fi
No password needed

Welcome to the NIST NCCoE



A collaborative hub convening experts from industry, government, and academia to solve organizations' most pressing cybersecurity challenges

The NCCoE's Impact

Strengthen U.S. Cybersecurity

Provide practical guides to implement standards-based, repeatable, and scalable solutions

Improve Technology

Help vendors strengthen products security and interoperability

Foster Public-Private Innovation

Convene industry, academia, and government to develop integrated solutions

Deliver Real-World Insights

Demonstrate solutions tested in real-world environments by leading cybersecurity experts

Support Standards Innovation

Reveal opportunities to improve standards to better address real-world challenges

IoT Open House: *Implementing SP 1800-36 and the Road Ahead*

Thursday, April 17, 2025
9:00 AM – 4:00 PM (EDT)



This session is being recorded

Morning Agenda

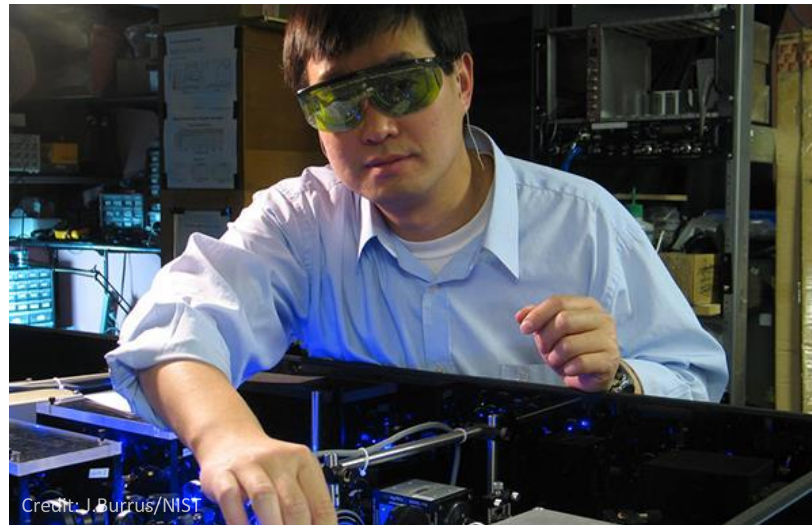
| Time (ET) | Session | Speaker(s) |
|-------------------|--|--|
| 9:00-9:30 AM | Arrival and Registration Check-In | |
| 9:30-10:00 AM | Welcome & Introductions | <ul style="list-style-type: none">• Michael Fagan, Principal Investigator, NIST NCCoE |
| 10:00 AM-12:00 PM | Parallel Technology Deep Dives – 25 minutes for deep dive presentations/discussion and questions with 5 min. transitions | <ul style="list-style-type: none">• Build 1: Dan Harkins, Aruba, an HPE company• Build 2: Darshak Thakore, CableLabs• Build 3: Michael Richardson (remote), Sandelman Software Works• Build 4: Brecht Wyseur (remote), Kudelski IOT• Build 5: Nick Allott, NquiringMinds• Factory Provisioning: Steve Clark, SEALSQ |
| 12:00-1:30 PM | Lunch (On your own) | |

Afternoon Agenda

| Time (ET) | Session | Speaker(s) |
|--------------|--|--|
| 1:30-2:30 PM | Technology Deep Dives (continued) | <ul style="list-style-type: none">• All Builds |
| 2:30-3:10 PM | Panel Discussion – Exploring Evolving Cybersecurity Threats and Challenges to IoT Devices | <ul style="list-style-type: none">• Michael Fagan - Moderator• Dan Harkins• Darshak Thakore• Nick Allott• Steve Clark• Zack Foreman |
| 3:10-3:55 PM | Discussion of Possible Next Steps/Follow-On Work for Application-Layer Project <ul style="list-style-type: none">• Matter• FIDO Device Onboarding (FDO) | <ul style="list-style-type: none">• Darshak Thakore, CableLabs, Matter Presenter• Brad Goodman, Dell Technologies, FIDO Presenter |
| 3:55-4:00 PM | Concluding Remarks | <ul style="list-style-type: none">• All |
| 4:00 PM | Adjourn | |

NIST Mission

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



Welcome to the NCCoE



Introduction to Trusted IoT Device Network-Layer Onboarding and Lifecycle Management Project

Speaker: Michael Fagan, Computer Scientist, NIST/NCCoE

Trusted IoT Network-Layer Onboarding: Objective

- Number of IoT devices is growing exponentially
 - Estimated 40 billion IoT devices
 - The growing number of IoT devices is leading to an expanding attack surface
 - We need scalable mechanisms to safely manage IoT devices throughout their life cycles
 - Network credential provisioning
 - Device intent
 - Device attestation
 - Application-layer onboarding
 - Additional zero-trust-inspired mechanisms

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



1. Device manufacture and factory provisioning

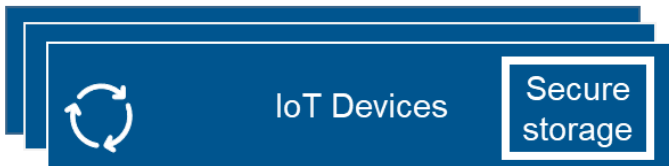
2. Device ownership and bootstrapping information transfer

Supply Chain
Integration Service

CA

Device Owner's Network

3. Trusted network-layer onboarding



Access Point, Router, or Switch

Network
Onboarding
Component

5. Continuous
verification

Continuous
Authorization
Service

4. Trusted
application-
layer
onboarding

Application
Server

Network-
Layer
Onboarding
Authorization
Service

Device
ownership
information
transfer

Device
bootstrapping
information
transfer

- **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

- **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).
- **Scenario 1: Trusted Network-Layer Onboarding**
 - Identities of the device and the network are authenticated.
 - The 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**

- Download 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.

Parallel Technology Deep Dives

Breakout Sessions

Please visit each Build Station at the color-coded times below that correspond to the sticker on your badge to help us ensure there is room for everyone in each session.

Build 1

10:00 – 10:25
(Red)

Room 5

Build 2

10:00 – 10:25
(Yellow)

Room 5

Build 5

10:00 – 10:25
(Blue)

Room 5

Factory Provisioning Build

10:00 – 10:25
(Green)

Room 5

Build 3

10:00 – 10:25
(Pink)

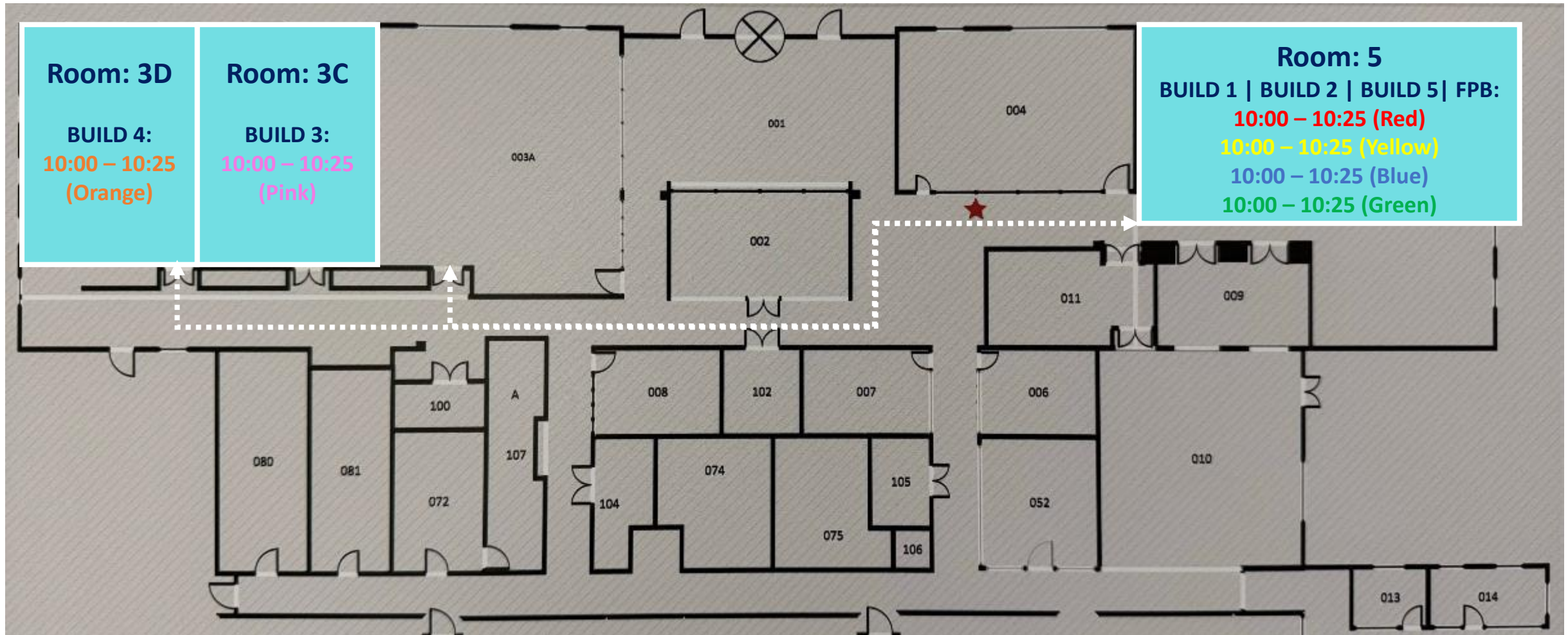
Room 3C

Build 4

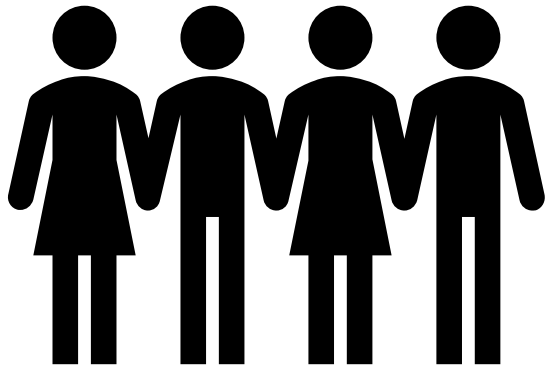
10:00 – 10:25
(Orange)

Room 3D

Work Session Locations



Lunch Break – 1 Hour 30 Minutes

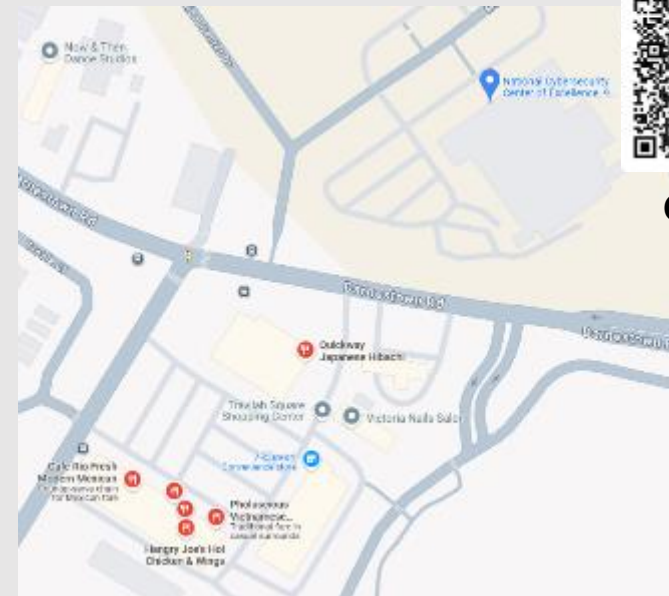


Next Up:
Parallel Technology
Deep Dives (continued)

12:00 – 1:30 PM
Off-site Options



Google Maps
Restaurants



Parallel Technology Deep Dives

Breakout Sessions

Please visit each Build Station at the color-coded times below that correspond to the sticker on your badge to help us ensure there is room for everyone in each session.

Build 1

1:30 – 1:55
(Blue)

Room 5

Build 2

1:30 – 1:55
(Green)

Room 5

Build 5

1:30 – 1:55
(Pink)

Room 5

Factory Provisioning Build

1:30 – 1:55
(Orange)

Room 5

Build 3

1:30 – 1:55
(Red)

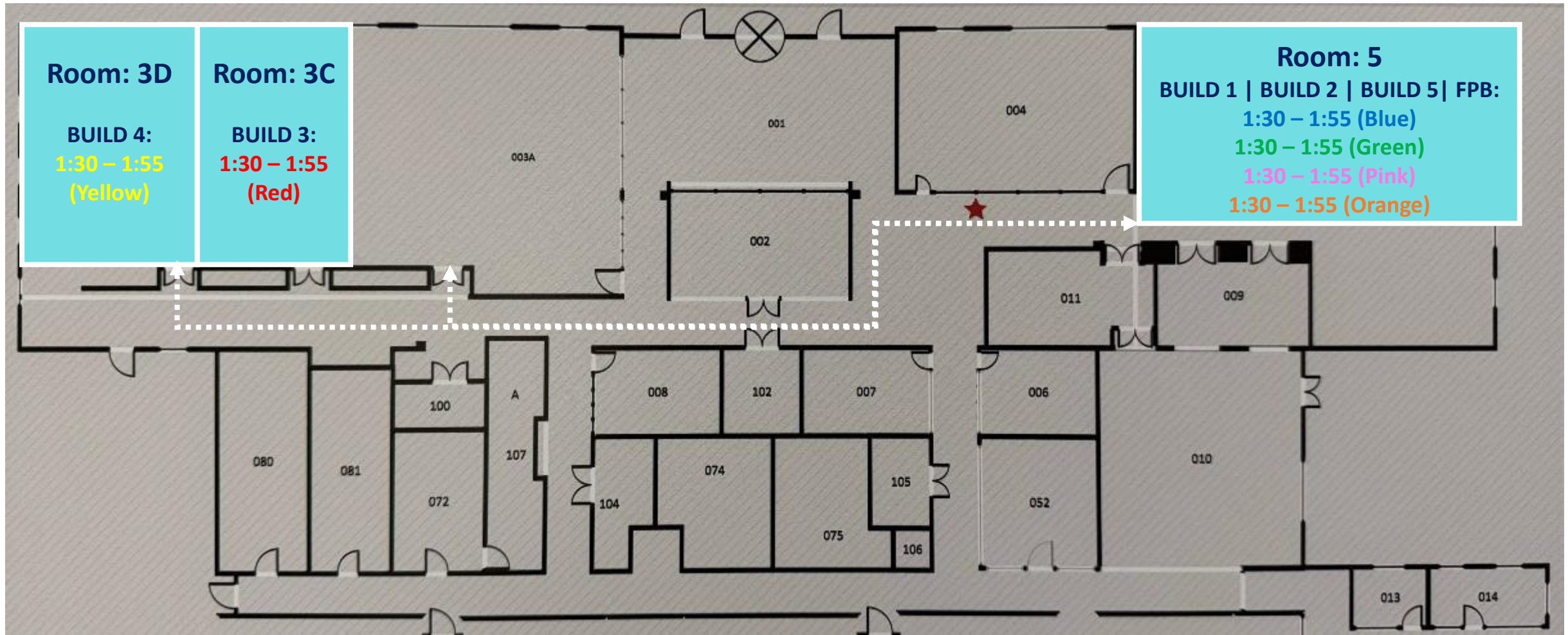
Room 3C

Build 4

1:30 – 1:55
(Yellow)

Room 3D

Work Session Locations



Panel Discussion

2:30 - 3:10 PM (EDT)

Panel Discussion: Exploring Evolving Cybersecurity Threats and Challenges to IoT Devices



**Michael Fagan
(moderator)**



Dan Harkins



**Darshak
Thakore**



Nick Allott



Steve Clark



**Zack
Foreman**

Discussion of Possible Next Steps

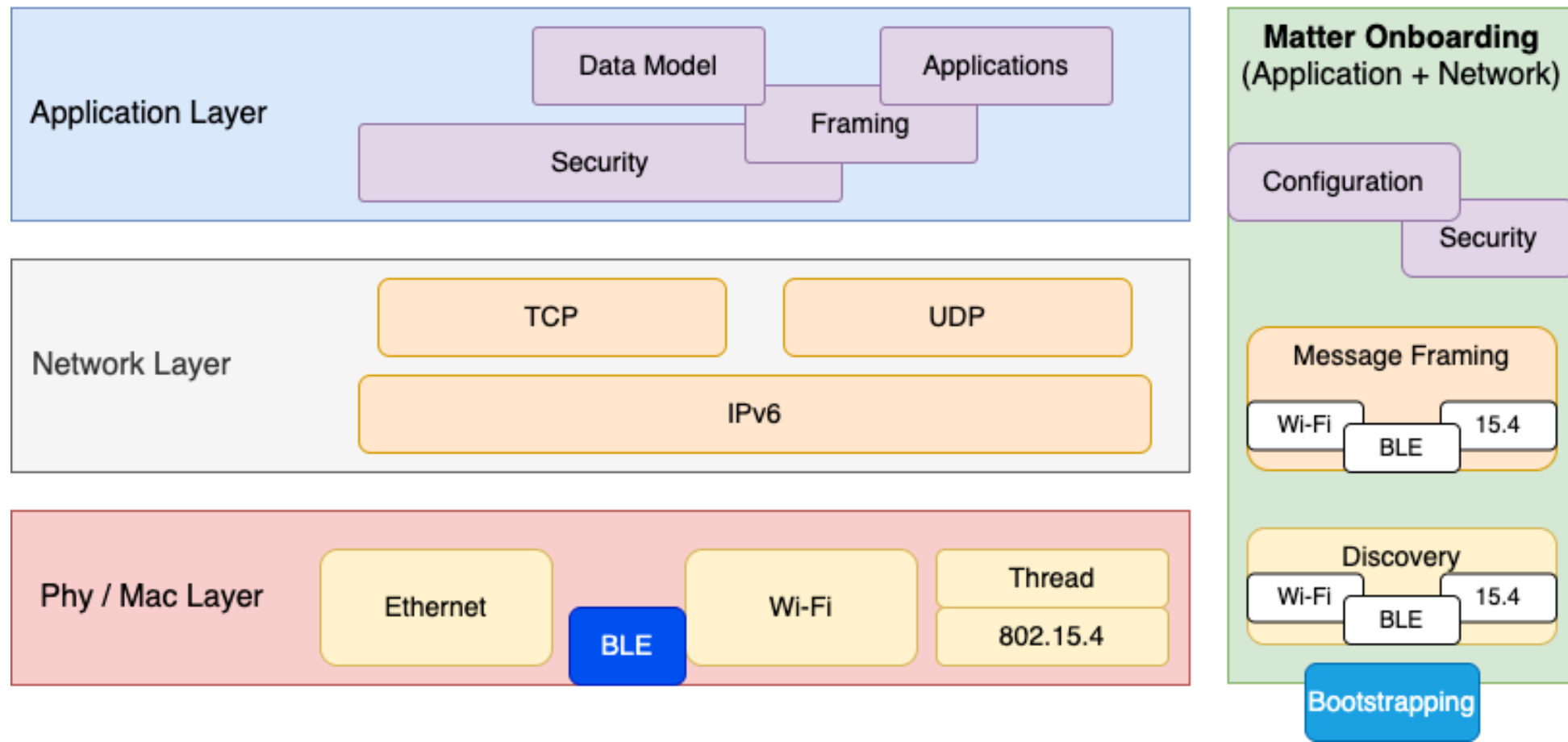
3:10 - 3:55 PM (EDT)

*Speaker(s): Darshak Thakore, Principal Architect, CableLabs
& Brad Goodman, Principal Engineer, Dell Technologies*

Matter

Matter Stack

The Matter protocol is expected to be run over different physical layers so network onboarding will be specific to the physical layer but the application layer onboarding is supposed to be agnostic to the underlying access layer



- Matter is primarily an application layer protocol
 - Strives to be “network agnostic”. However..
 - Network layer onboarding is “network specific”
 - And hybrid.... Configure Wi-Fi over BLE or Ethernet, Thread over IP
 - No “clean” solution available (at the time)
- Matter adoption
 - Gaining traction in the ecosystem
 - May not always be the “primary” protocol used by the user

Discussion points (open questions)

- Does the evolution/adoption of Matter impact the high-level architecture (slide 12)
 - What (if anything) would we consider differently?
- How do we get secure network layer onboarding to “fit well” with various application layer stacks
 - Is there opportunity for any standardization here ?
 - Or maybe some guidelines/best-practices
- How do we “address” Matter in SP 1800-36

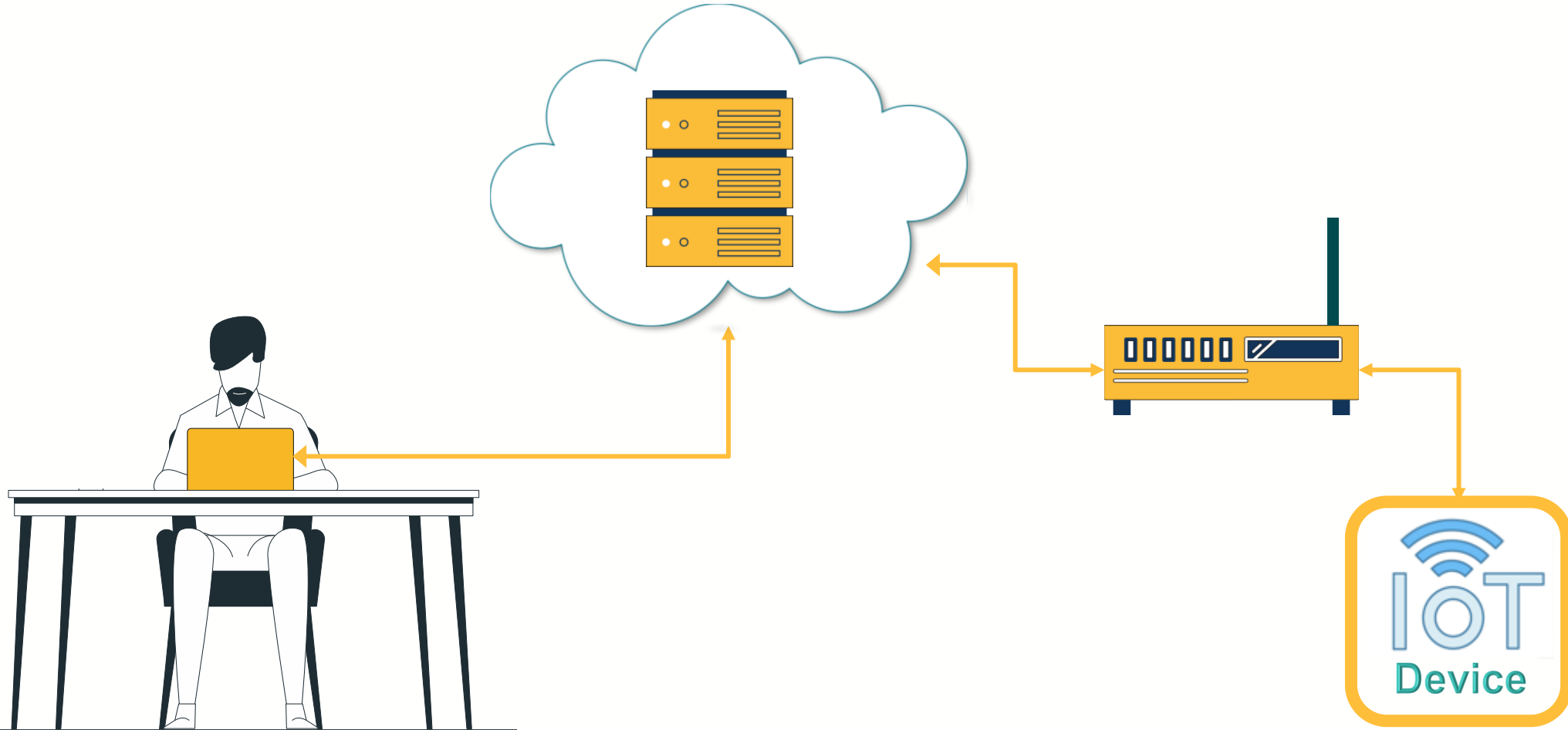


Foundational Cybersecurity Activities for IoT Device Manufacturers

Leveraging FIDO Alliance cybersecurity
standards in support of IR8259



Major elements of an IoT system

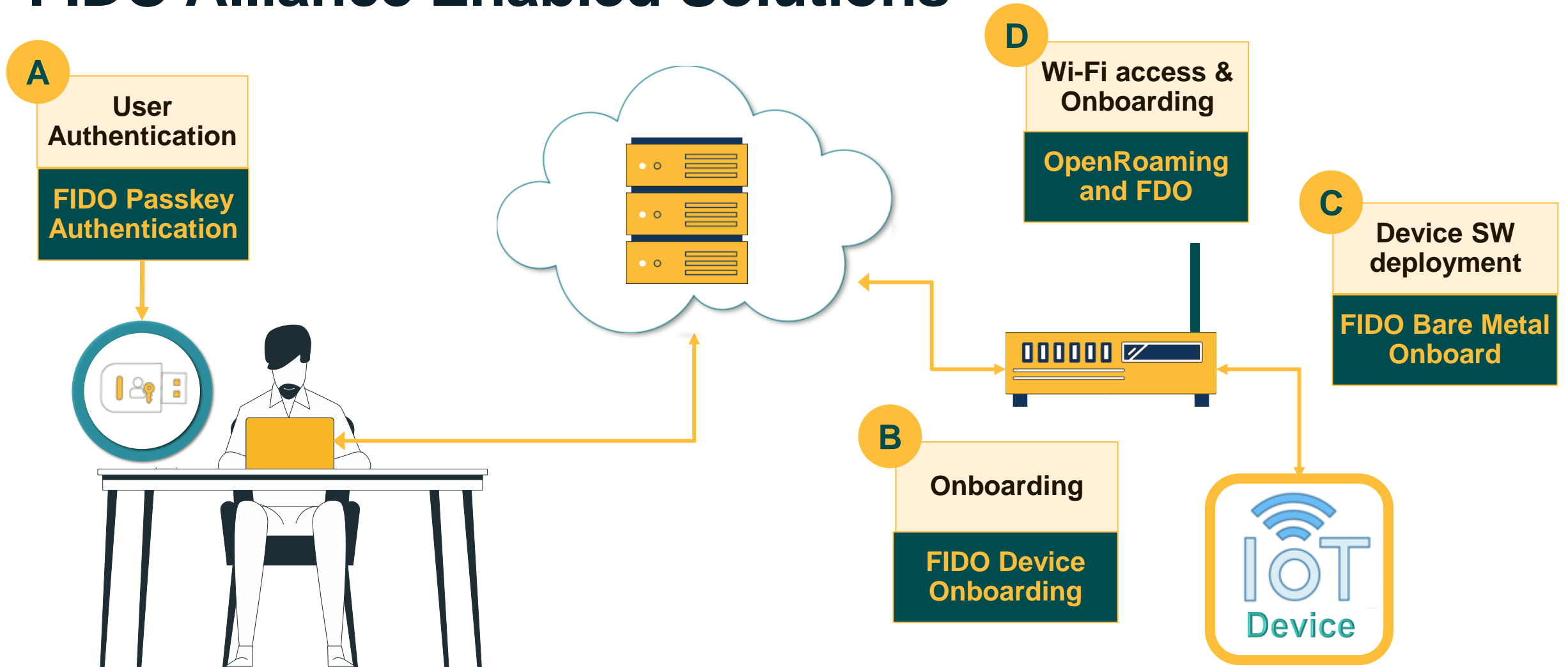


IoT Challenges

From a cybersecurity viewpoint, IoT products must provide:

1. **Secure Communication:** Enable encrypted, reliable data transmission.
2. **Private Data Access:** Safeguard sensitive IoT data for users.
3. **Management Connectivity:** Provide secure onboarding to on-site or cloud platforms.
4. **Robust & Upgradable Software:** Ensure resilience, updates, and cybersecurity.
5. **Recovery Mechanism:** Restore to a secure baseline in emergencies.

FIDO Alliance Enabled Solutions



Passkeys

What is a passkey?

Passkey

/ˈpas, kē/ noun

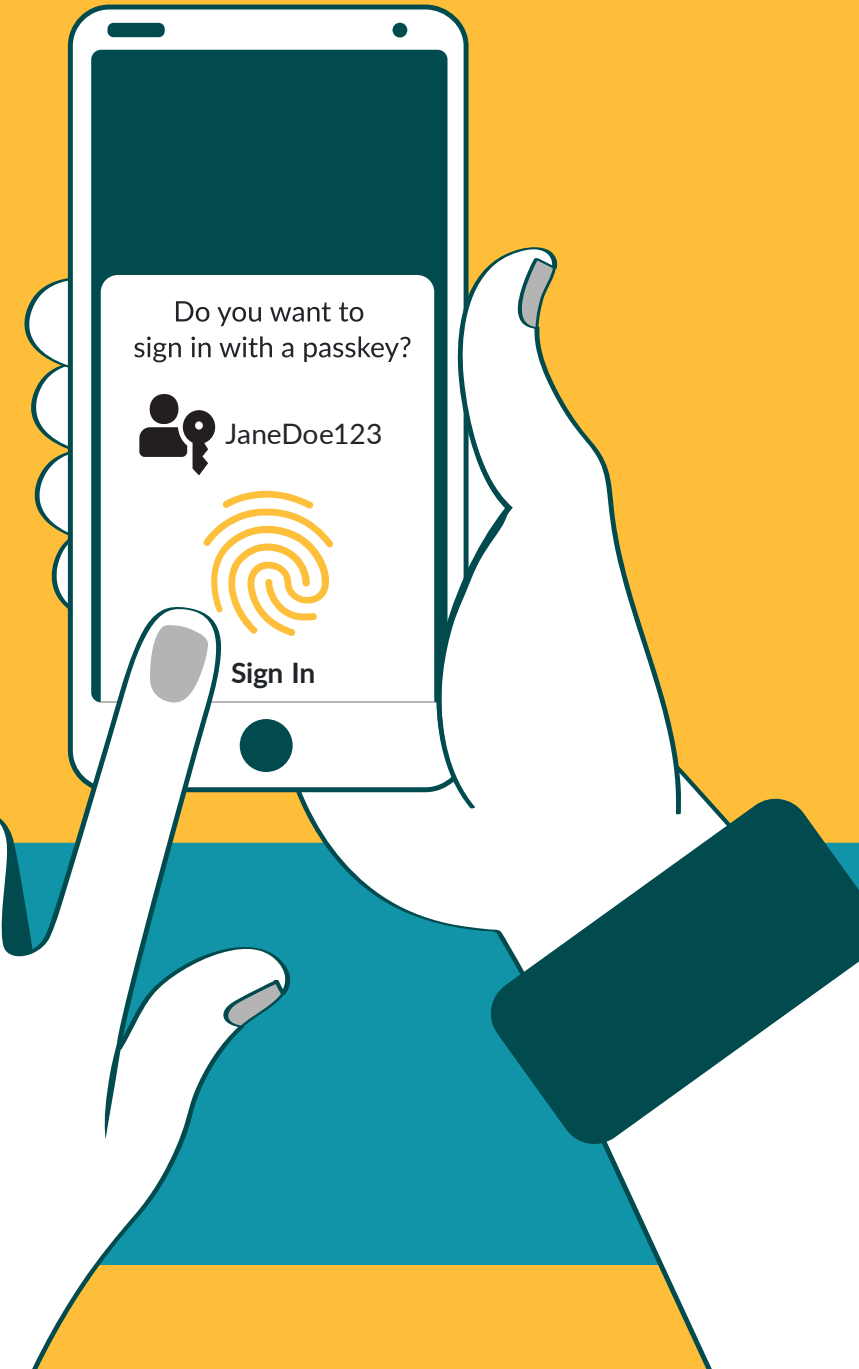
Passkeys are a password replacement based on FIDO protocols that provide faster, easier, more secure sign-ins to online services.

A passkey may be synced across a secure cloud so that it's readily available on all of a user's devices, or it can be bound to a dedicated device such as a FIDO security key.

4x simpler

Passkeys are 4x simpler to use since they don't need to be remembered or typed. You just use your fingerprint, face scan, or screen lock to sign in across all your devices and platforms.

Source: Google

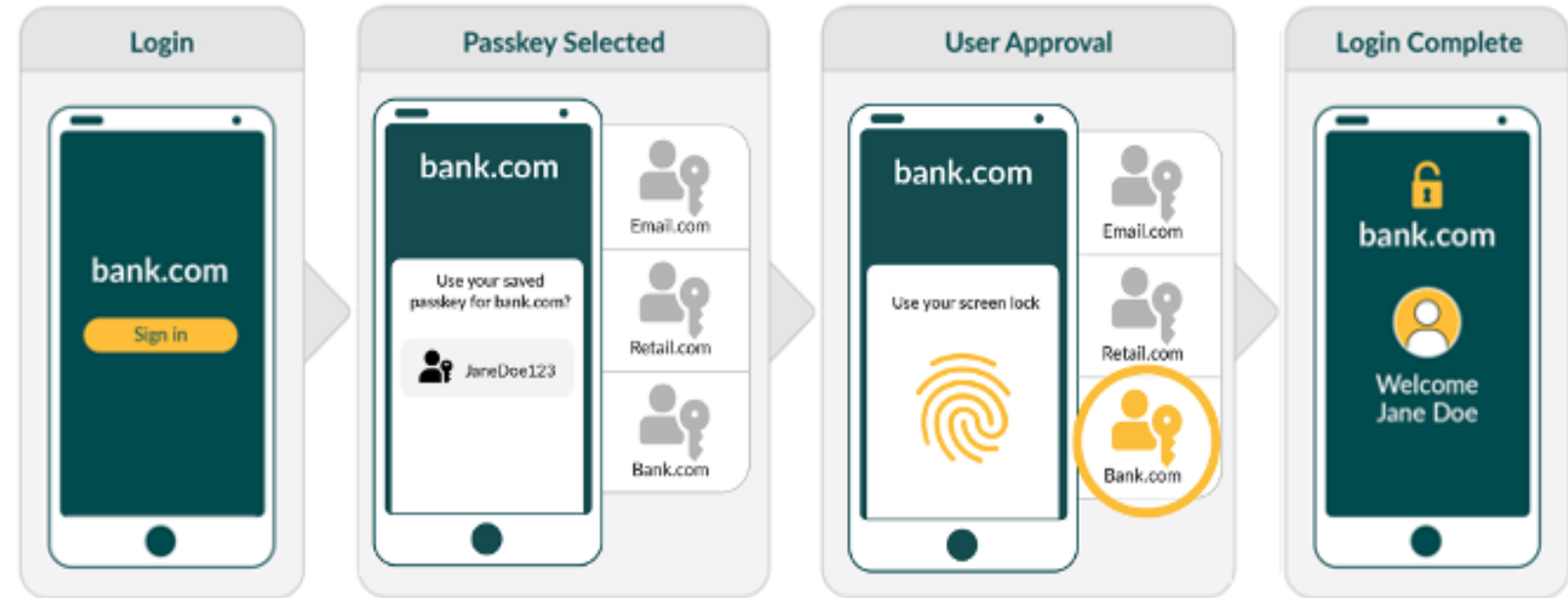


How Passkeys Work

Simplest and fastest way to sign-in

Passkeys are 4x simpler to use since they don't need to be remembered or typed.

With a fingerprint, face scan, or screen lock, users can sign in across all their devices and platforms.



A passkey has 2 parts: the user's private key that corresponds to their devices, and a public key on the server to authenticate with the service provider.

When a user signs in, the service provider checks to see if the public key matches the user's private key.

To verify their identity with the service provider, the user is prompted to unlock their device with their private passkey.

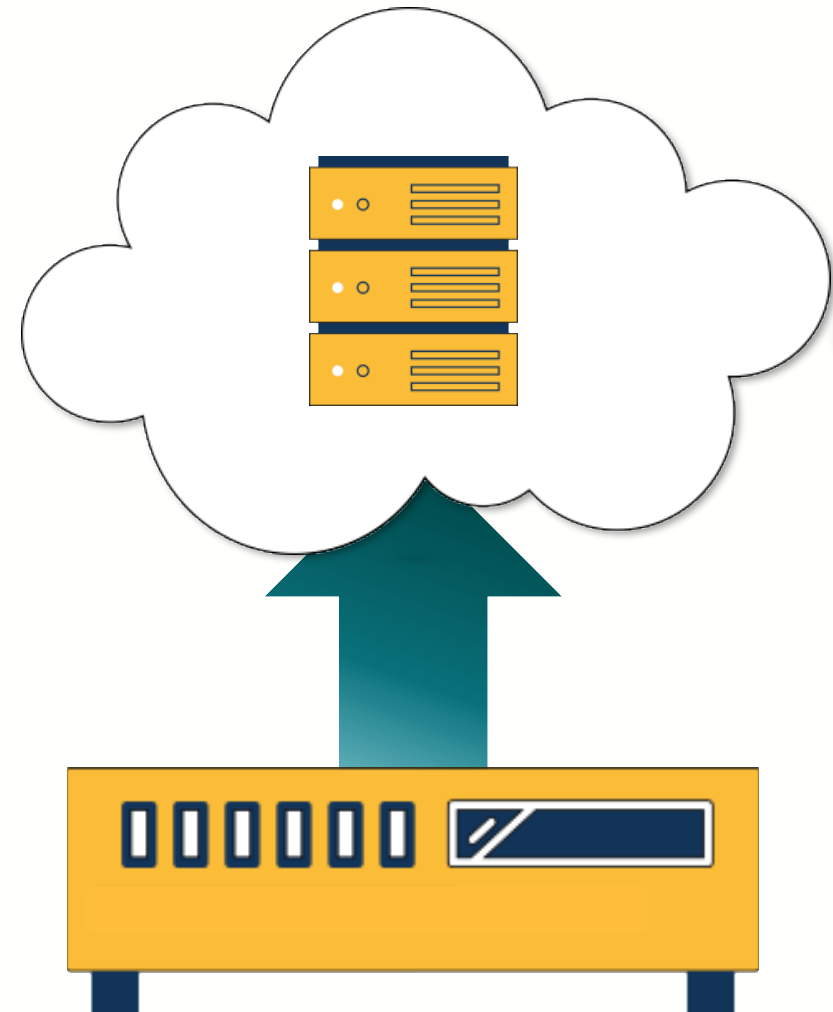
The private key is private to the user and is not visible to their credential manager or the service they are signing into.

source: <https://fidoalliance.org/how-fido-works/>

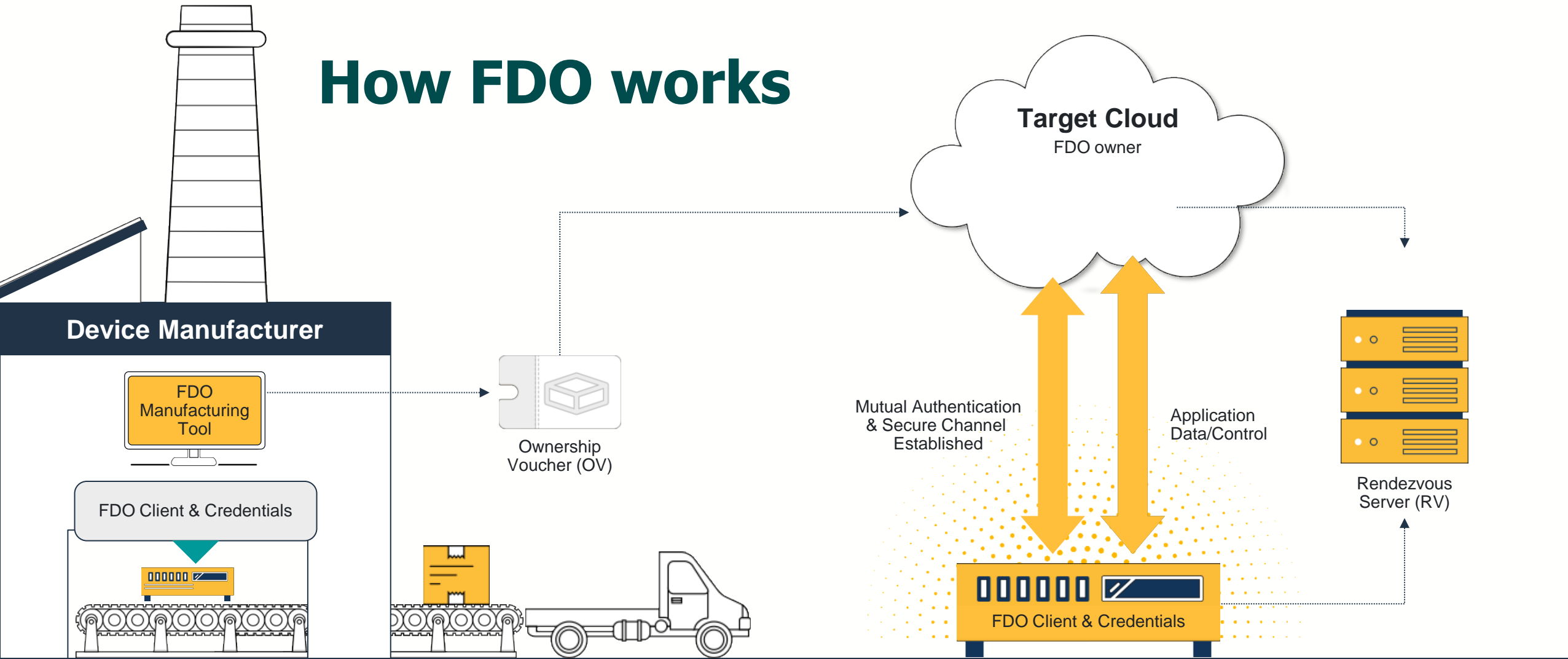
FIDO Device Onboard (FDO)

What problem does FIDO Device Onboard (FDO) solve?

- When an Edge or IOT solution is being installed in a facility, the device must be “onboarded” to its management platform (on-premise or cloud).
- FDO provides secure “plug and play” onboarding for almost any device/network.



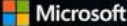
How FDO works



Microsoft presented Azure Edge at Ignite



[Link to all Workshop videos](#)



Who were?

Azure Edge Infrastructure


Simplifying Edge Deployments with Azure Arc and FIDO Device Onboarding

Gerardo Diaz Cuellar


Principal Software Engineer


Gerardo Diaz Cuellar

Partner Software Engineer Architect



Gerardo Diaz Cuellar
Microsoft



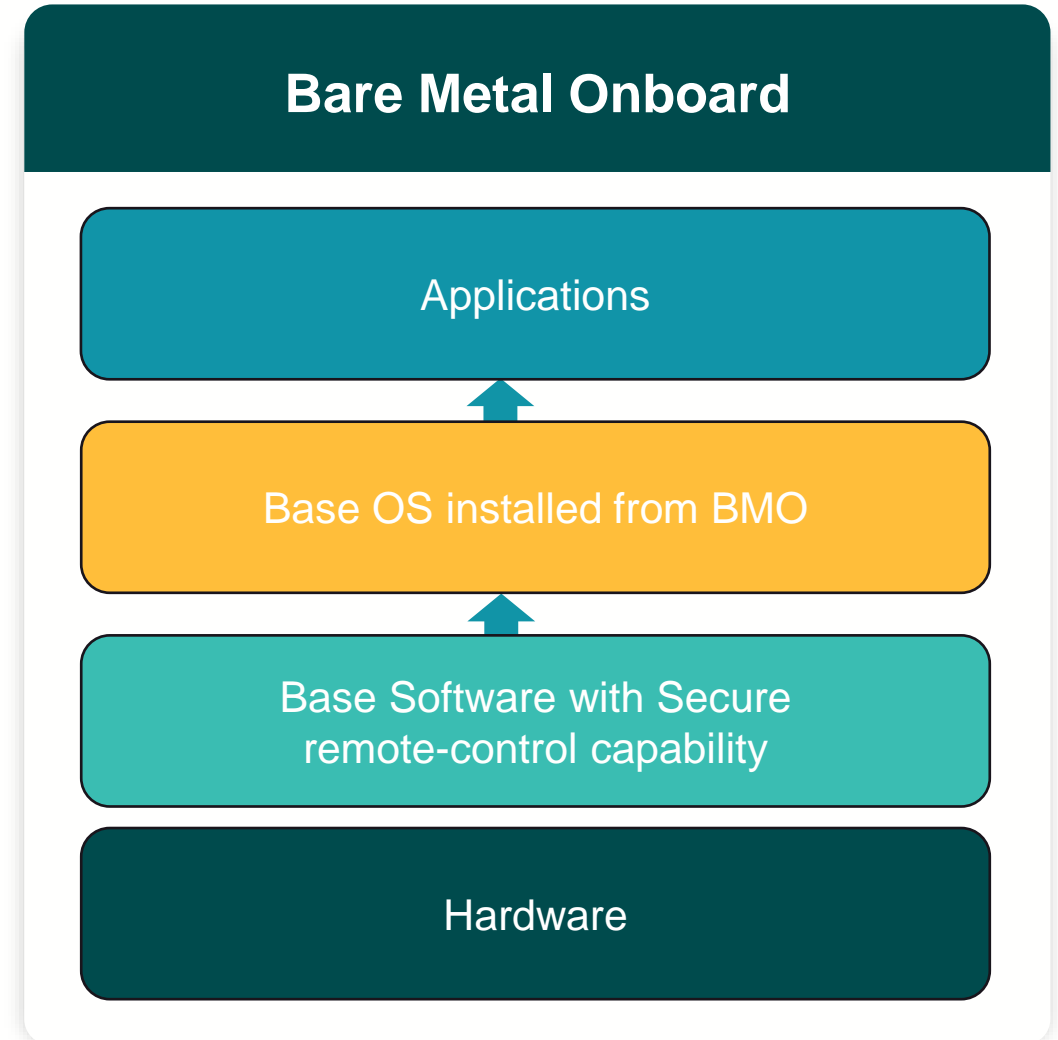


Moving forward – Bare Metal Onboard (BMO)

Please note that this section reflects the current thoughts of the FIDO Working Group but is not POR

Bare Metal Onboard

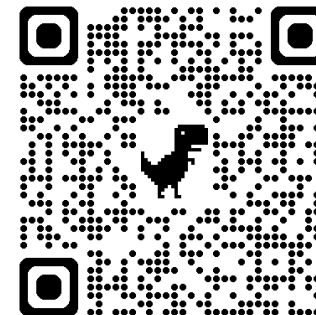
- The FIDO Onboarding working group is now planning extensions to FIDO that will allow ‘**bare metal onboarding**’ – **BMO**.
- BMO will allow general-purpose IoT/Edge devices to be built without any knowledge of end-purpose/application.
- This provides a consistent and deterministic way of Late Binding the entire state of a system
- Delivers an ‘any OS to any Device’ experience.



OpenRoaming with Onboarding

OpenRoaming for IoT – FIDO Device Onboarding Framework

- The **Wireless Broadband Alliance** (WBA) and the FIDO Alliance have joined forces to integrate **FIDO Device Onboard** (FDO) and WBA OpenRoaming™ technologies.
- This collaboration aims to create a seamless and secure onboarding process for Internet of Things (IoT) Wi-Fi devices.
 - Zero-touch, secure onboarding
 - OpenRoaming and FDO integration
 - Alternative network environments
 - Supply chain security



Thank you

Read Our Recent Publications:

NIST Cybersecurity White Paper (CSWP)

42: [Towards IoT Security: Implementing Trusted Network-Layer Onboarding](#)

NIST SP 1800-36: [Trusted IoT Device Network-Layer Onboarding and Lifecycle Management](#)

View Our Full Portfolio of Work:

[NCCoE IoT | nist.gov](#)



✉ IoTOnboarding@nist.gov



 nccoe@nist.gov



nccoe.nist.gov



[@NISTcyber](https://twitter.com/NISTcyber)

Adjourn