Peace of Mind for IoT embedded designers

A Secure end-to-end Reference Design

Ali Sebt

SEBTRONIX Business Group, Inc.

IoT and Security

- Embedded designers are experts in Operation Technology (OT)
  - Safety
  - Sensor Control
  - Actuator Control
  - Power Management
  - Ultra low power consumption

IoT and Security

- Embedded designers are experts in Operation Technology (OT)
  - Safety
  - Sensor Control
  - Actuator Control
  - Power Management
  - Ultra low power consumption

- With the proliferation of IoT
  - Connected machines and their Operation Technology functionality are creating vulnerabilities for IT infrastructures

OT: Target of Cybersecurity Hacks & Attacks

Thousands of OT Vulnerabilities every month

Mechanical contractor hacked to steal
a major department store's client information

Important Notice: unauthorized access to payment card data in U.S. stores

December 19, 2013

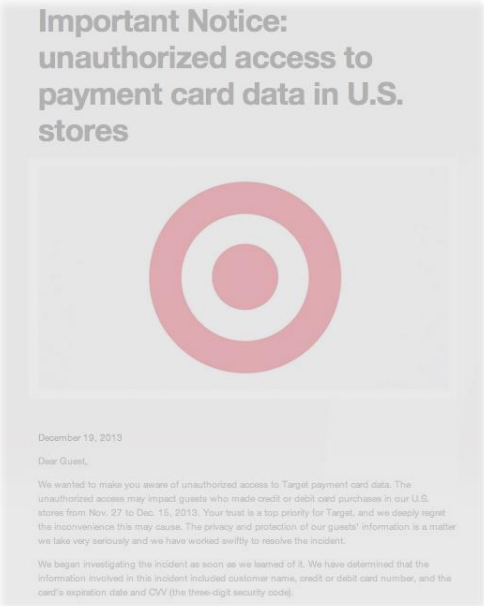
Dear Guest,

We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.

We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV (the three-digit security code).

Thousands of OT Vulnerabilities every month

Mechanical contractor hacked to steal
a major department store's client information


Important Notice: unauthorized access to payment card data in U.S. stores

December 19, 2013

Dear Guest,

We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.

We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV (the three-digit security code).

A casino lobby connected fish tank
thermometer hacked to steal client information

PSAcertified.org for IoT H/W, S/W & Devices

…”on average there are 5,400 attacks per month on IoT devices, with 7 million data records compromised daily.”

“The average cost of a successful IoT device attack is more than $330,000 and … by 2025 cybercrime damages will total $10 trillion.”

https://www.psacertified.org/what-is-psa-certified/why-choose-psa-certified/

IoT and Security

- Some believe that because their machines have not been hacked, then their systems work just fine

IoT and Security

- Some believe that because their machines have not been hacked, then their systems work just fine

- Some rely on the security of the transport layer

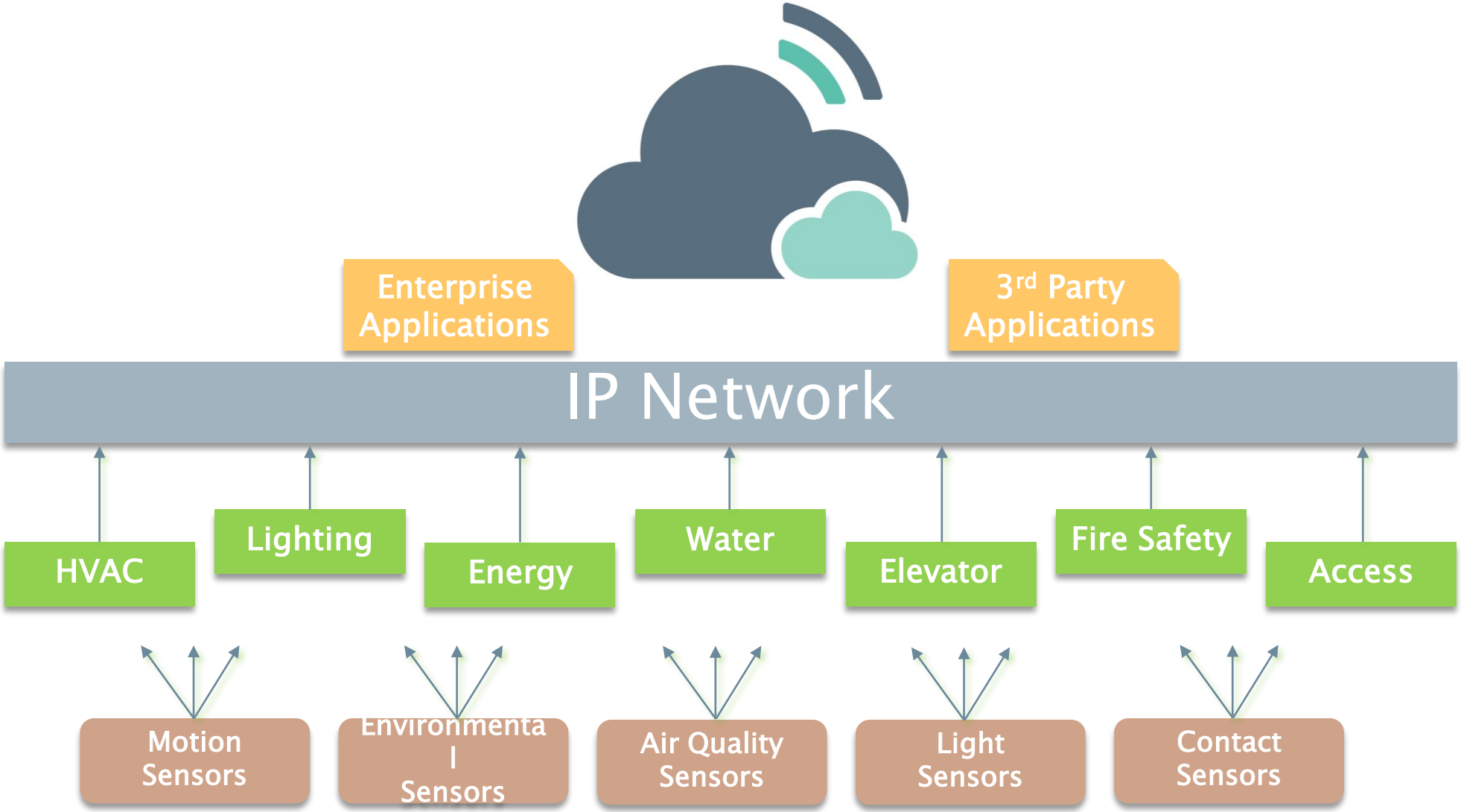
IoT and Security

- Some believe that because their machines have not been hacked, then their systems work just fine
- Some rely on the security of the transport layer
- The opportunity is to secure the data and intelligence at the device level

IoT and Security

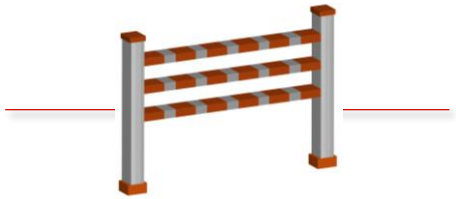
- Some believe that because their machines have not been hacked, then their systems work just fine
- Some rely on the security of the transport layer
- The opportunity is to secure the data and intelligence at the device level
- This will protect everyone in the value chain

Infrastructures Adopting IoT at Rapid Pace

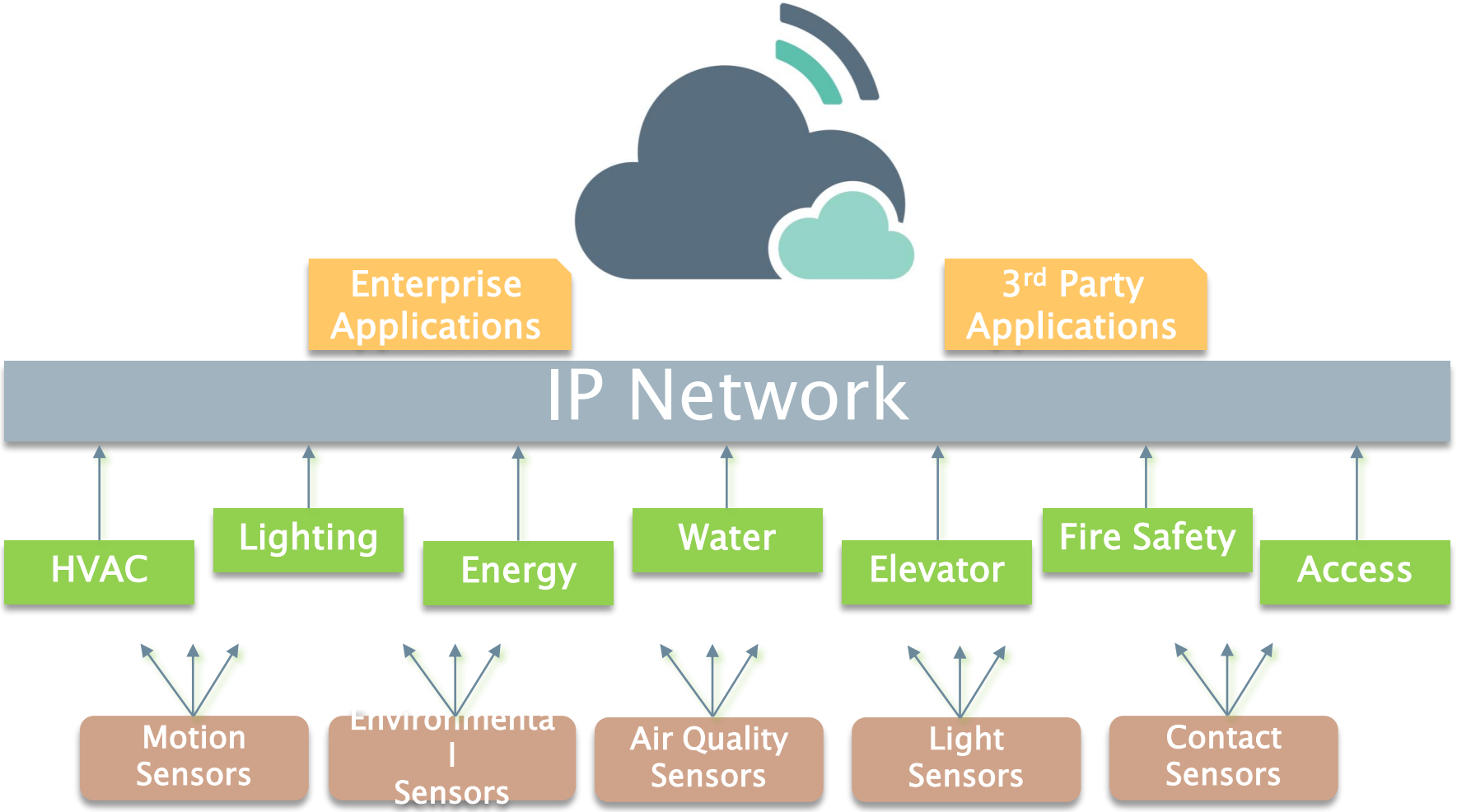


Barrier to Entry

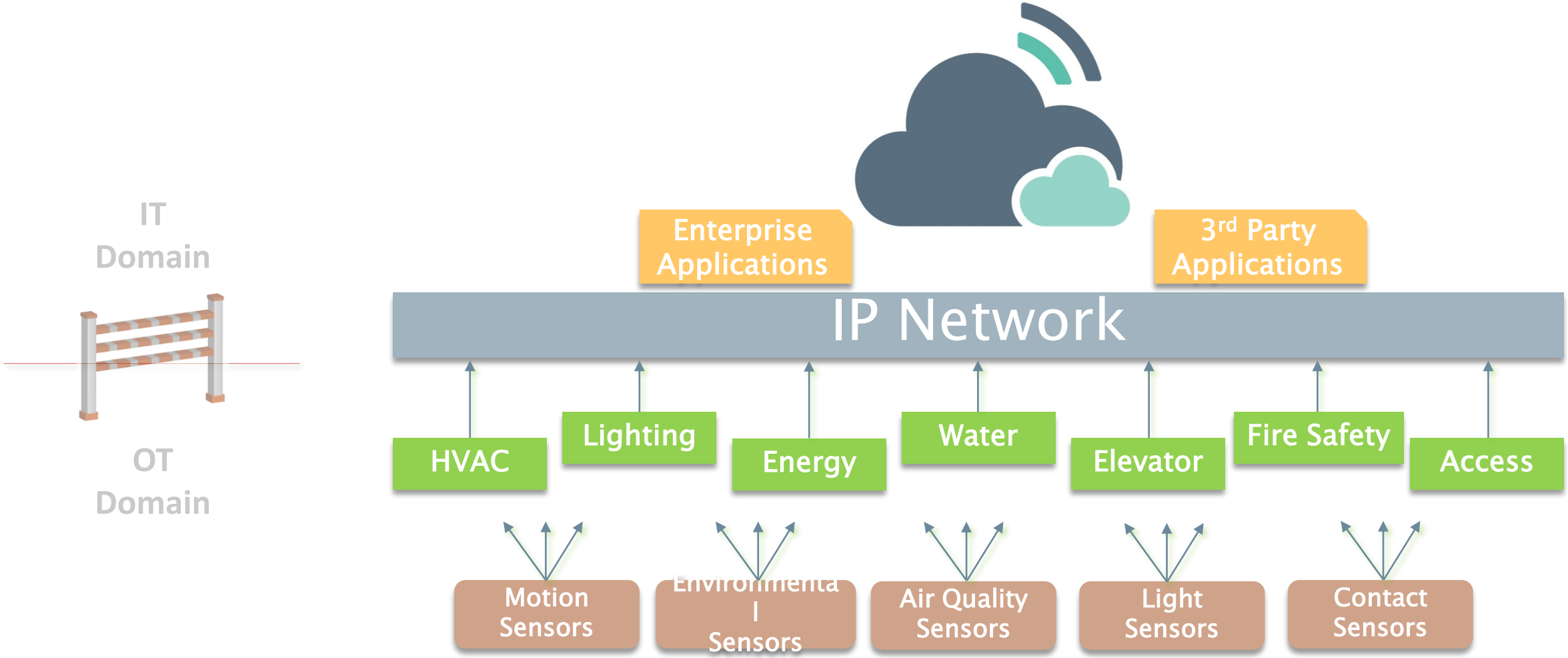
IT Domain



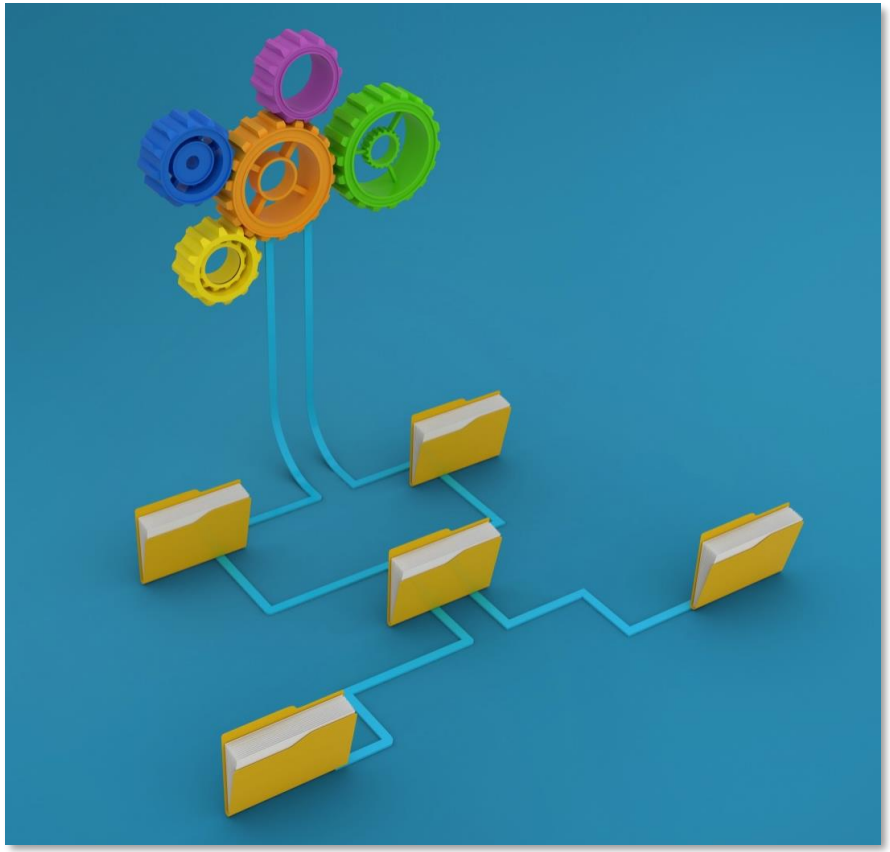
OT Domain



IT & OT Domains Integrated in the Cloud

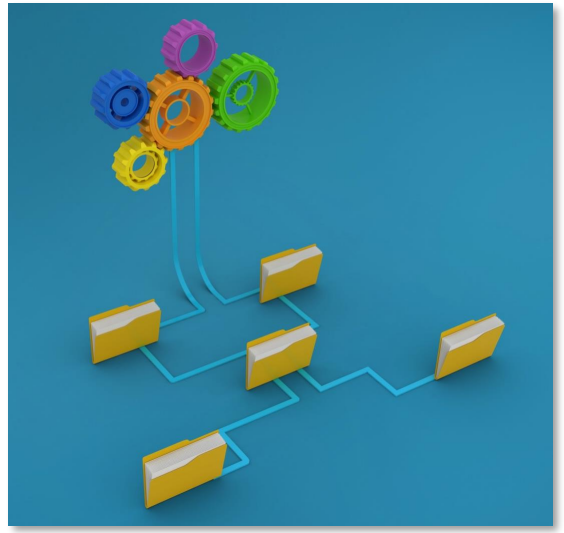


Device LifeCycle Management



Device LifeCycle Management (DLM)

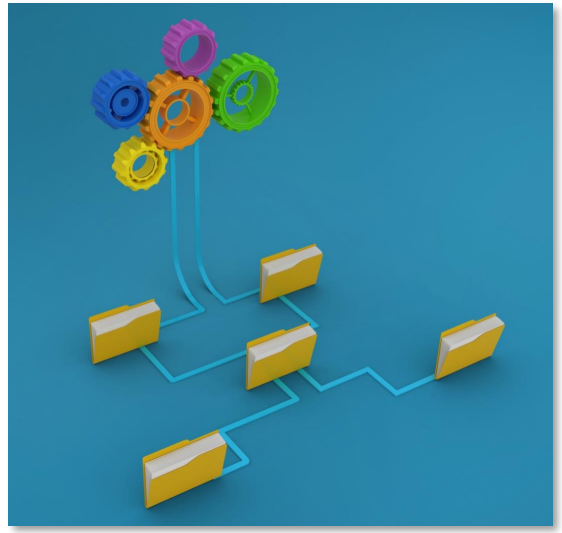
1. Onboarding



Device LifeCycle Management (DLM)

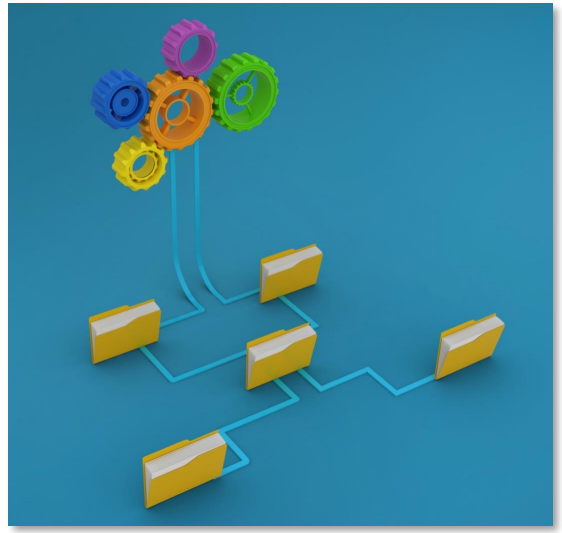
1. Onboarding

2. Configuration & Control

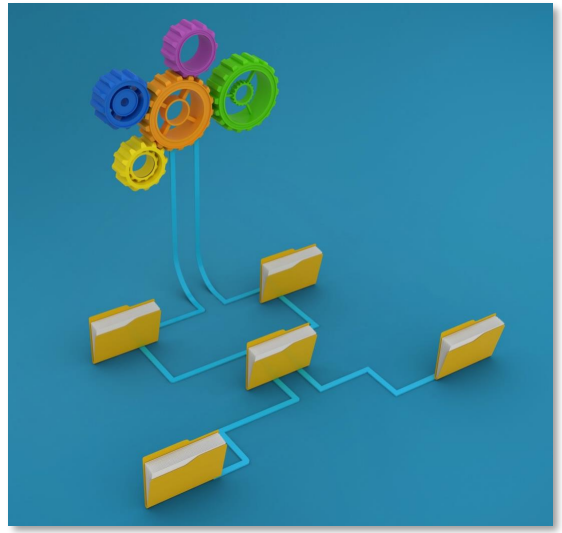


Device LifeCycle Management (DLM)

1. Onboarding
2. Configuration & Control
3. Ongoing Monitoring, Alerts & Diagnostics

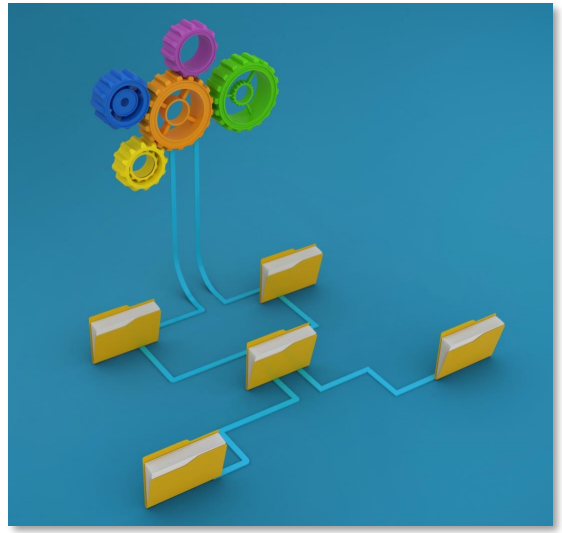


Device LifeCycle Management (DLM)



1. Onboarding
2. Configuration & Control
3. Ongoing Monitoring, Alerts & Diagnostics
4. Maintenance & Over-the-Air (OTA) Updates

Device LifeCycle Management (DLM)

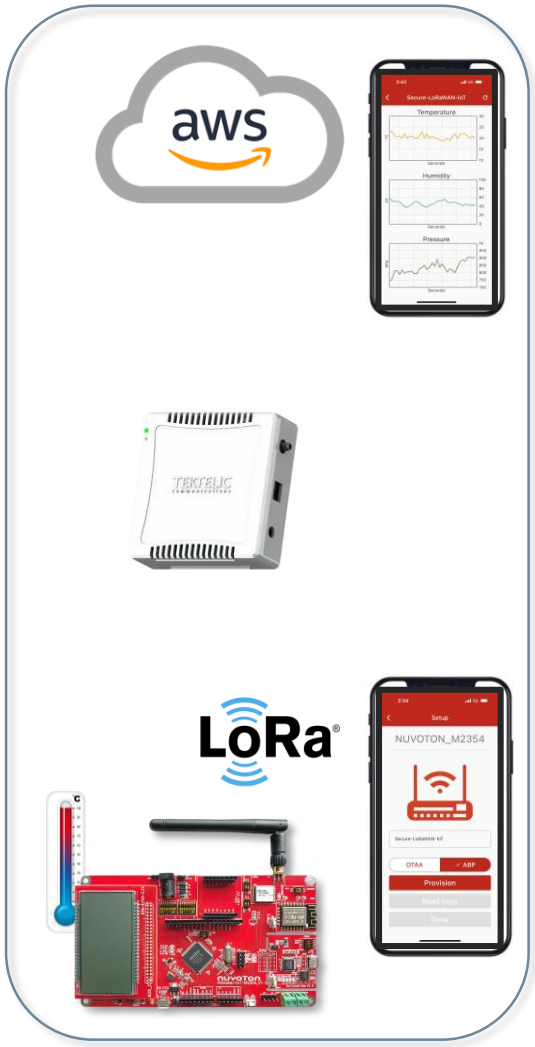


1. Onboarding
2. Configuration & Control
3. Ongoing Monitoring, Alerts & Diagnostics
4. Maintenance & Over-the-Air (OTA) Updates
5. Decommissioning & Sunsetting

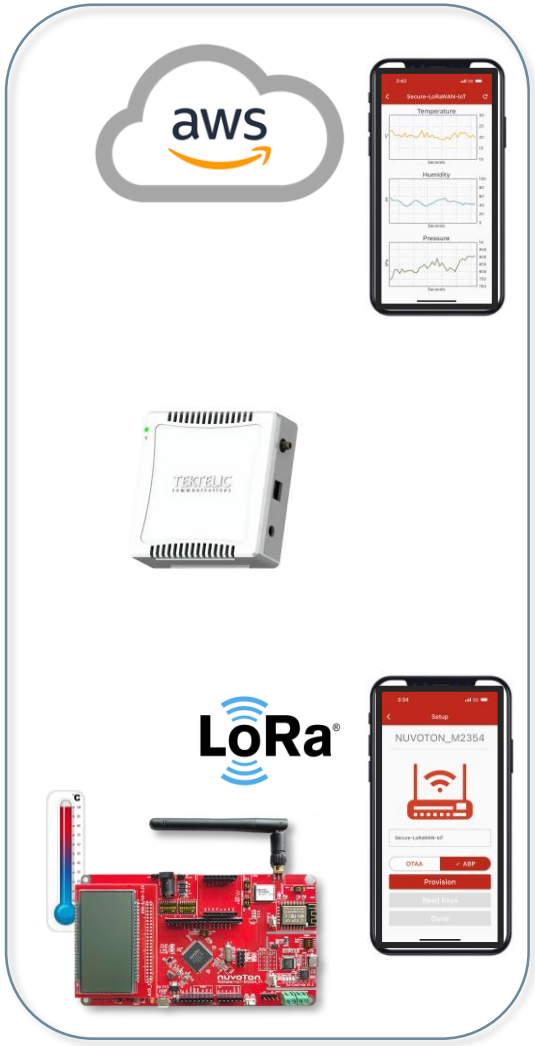
Connected Exercise Machine

1. Onboarding
2. Configuration & Control
3. Ongoing Monitoring, Alerts & Diagnostics
4. Maintenance & Over-the-Air (OTA) Updates
5. Decommissioning & Sunsetting

Secure end-to-end IoT Reference Design



Objective: To Simplify Secure Provisioning



Components of the Reference Design

A Global IDH Ecosystem Partner

ECOSYSTEM

DORNERWORKS

Complete ***Device to Cloud*** Development

Secure Embedded Technologies

FDA Compliant ***Medical Device*** Development

Accelerated Processing (***FPGA***)

Grand Rapids, Michigan

NuMicro M2354 Secure MCU

Security

ARM® TrustZone®

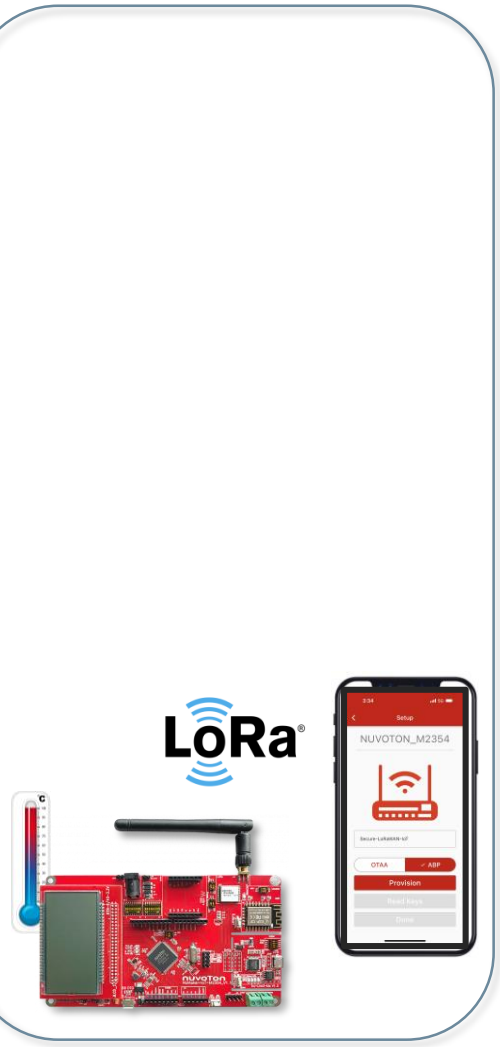
KeyStore

Cryptographic Hardware Accelerator

NuMaker IoT M2354 Board

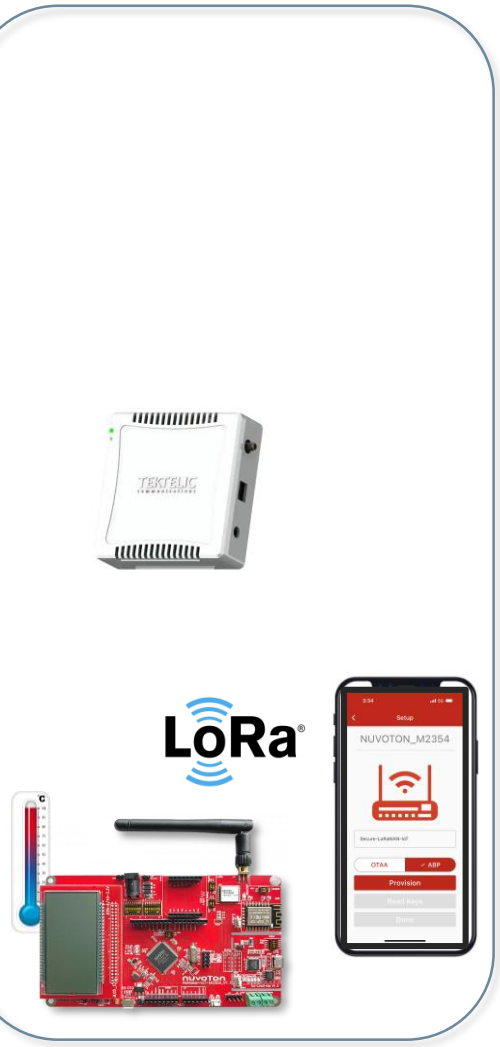
- M2354 Cortex-M23 MCU with ARM® TrustZone®
- Environmental Sensor
- LoRaWAN® via Semtech Radio
- WiFi via ESP module
- BLE added via Click9 module
- On-Board Debugger

Mobile App for Provisioning



- iOS & Android
- Onboarding of Authorized Installers & Users
- Provision Devices to Cloud
- Device Management

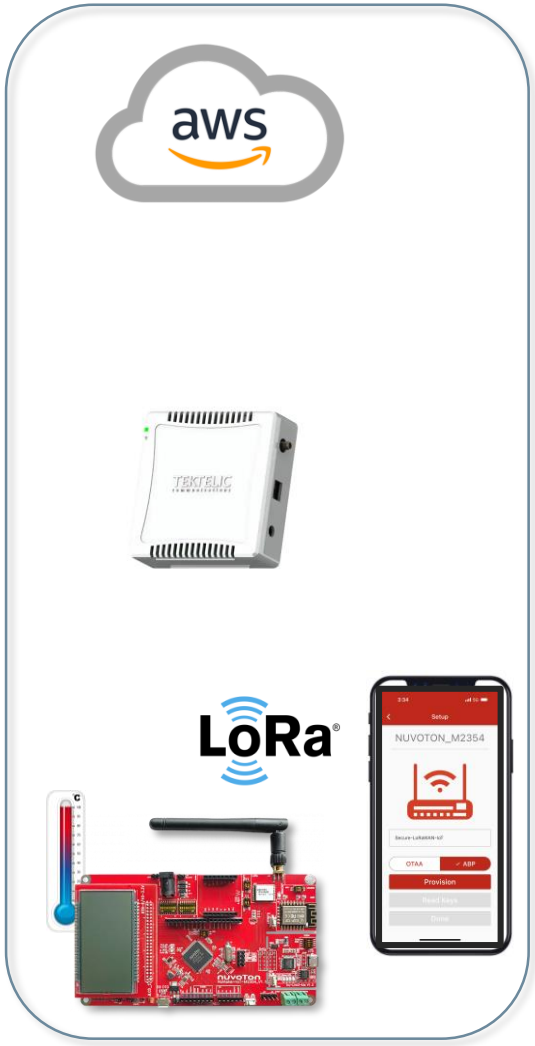
TEKTELIC LoRaWAN® Gateway



- Integrated Cellular 3G/4G
- Ethernet backhaul
- NA 915, EU868, JP920 ISM Frequency Bands

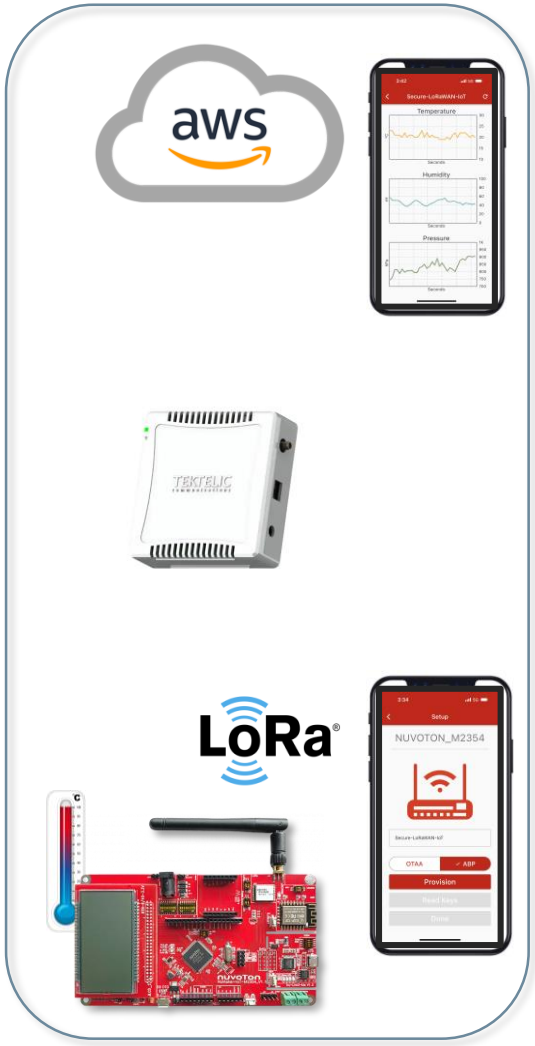
* TEKTELIC Gateway is sold separately

Cloud Applications



- AWS IoT Core: LoRaWAN® Network Server
- AWS Cognito: User management

Mobile App to Display Sensor Data



- iOS & Android
- Temperature, Humidity, Pressure

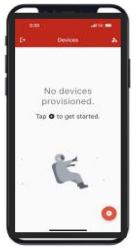
The Out-of-Box Experience

The Out-of-Box Experience

The Device will Come Up in BLE Broadcast Mode

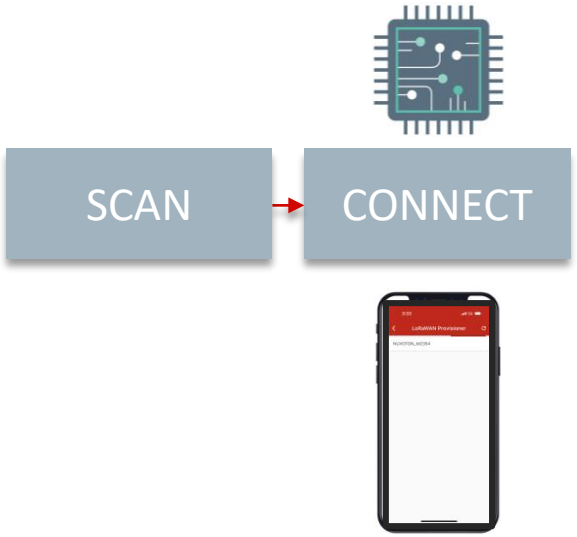
User will Scan for Device

SCAN



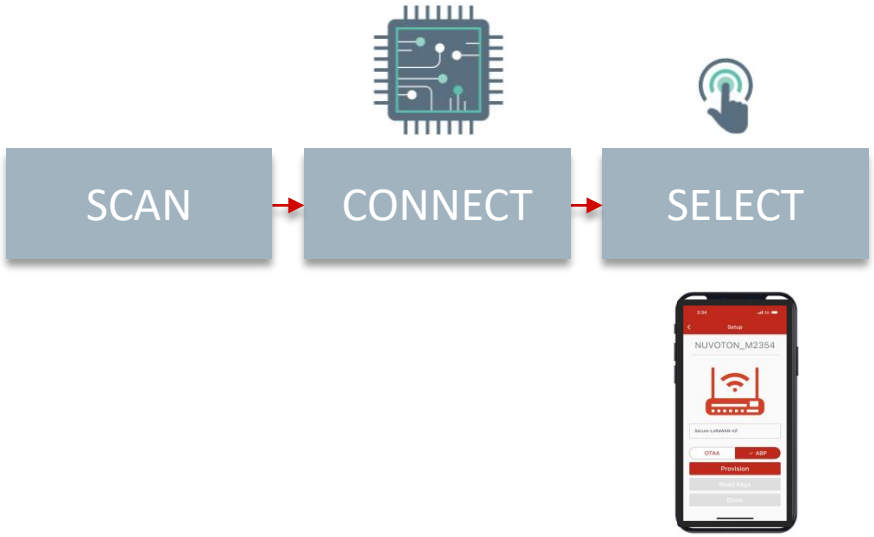
The Out-of-Box Experience

Then the App will connect to the Device



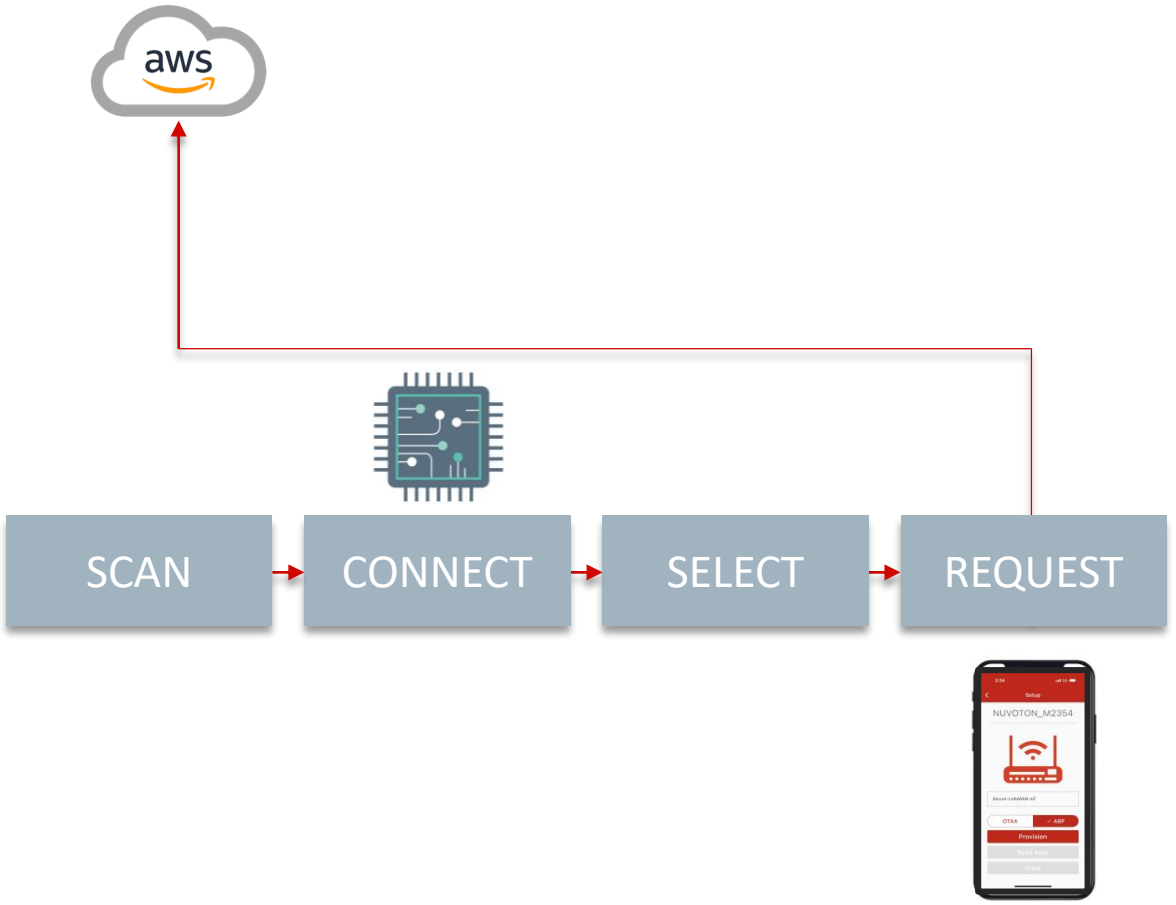
The Out-of-Box Experience

Then on the App, you select the provisioning Key type



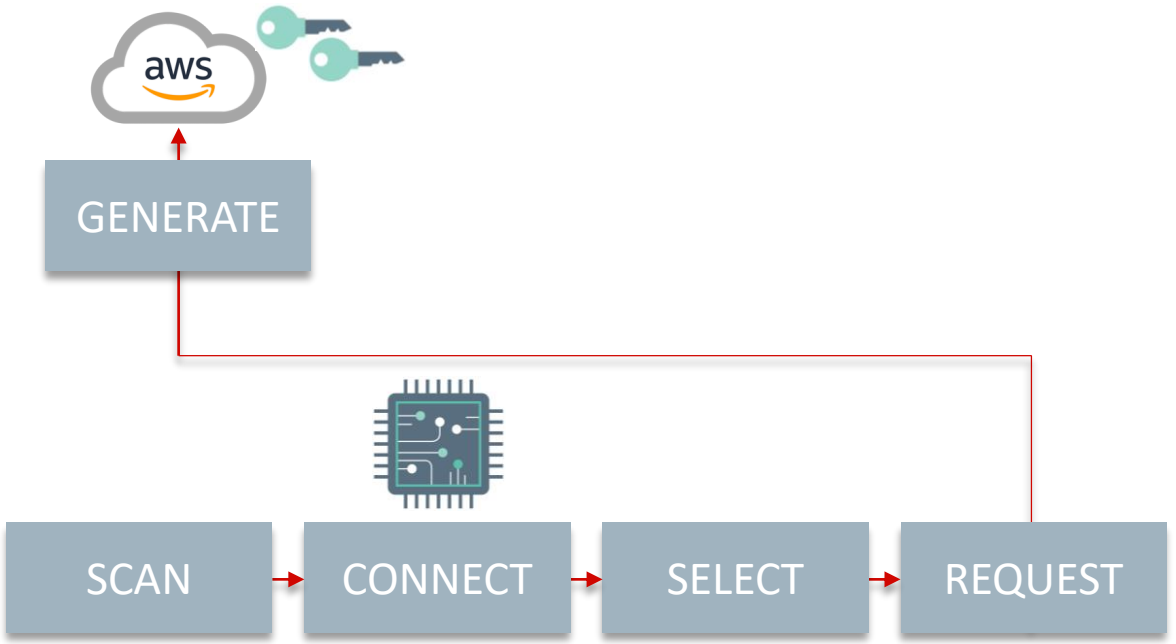
The Out-of-Box Experience

The App will make Key requests from both the Network server and the Application server



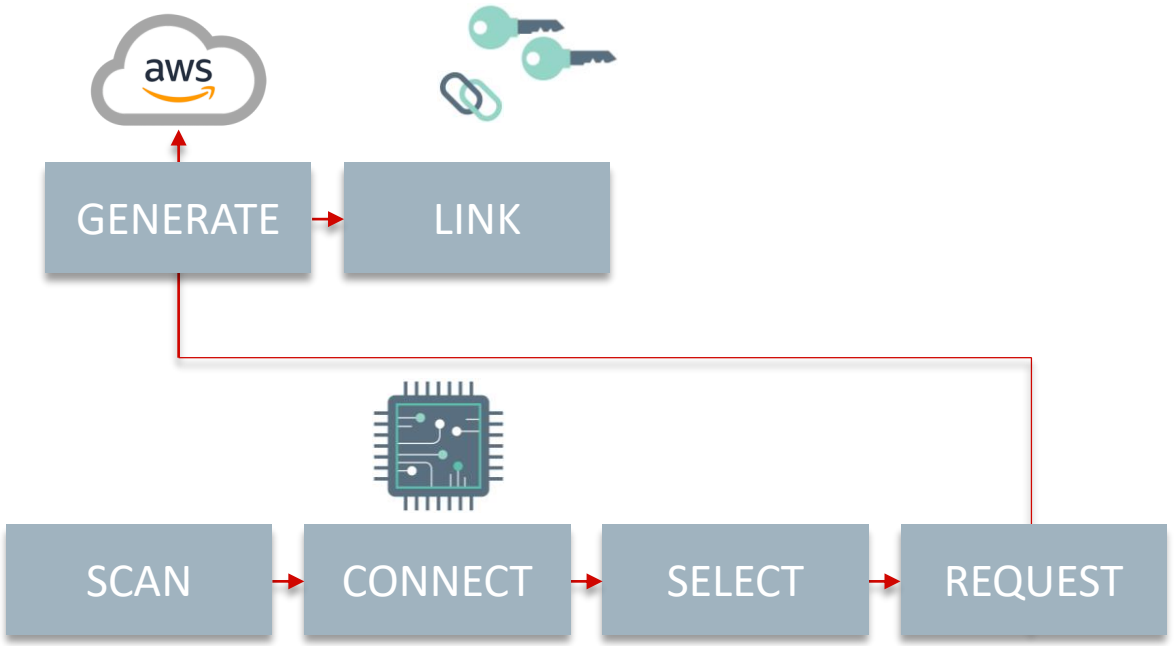
The Out-of-Box Experience

Then the servers will generate the provisioning Keys



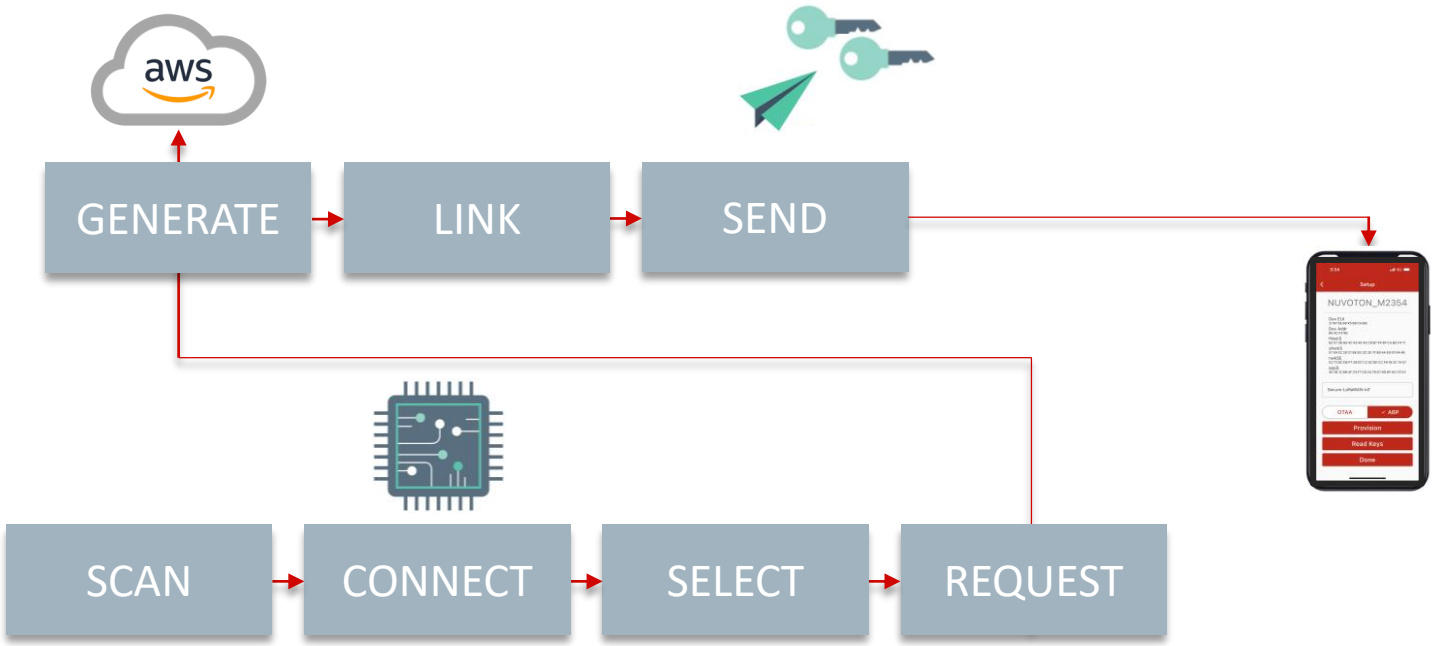
The Out-of-Box Experience

Next the Application server will link the Device to the User's Account



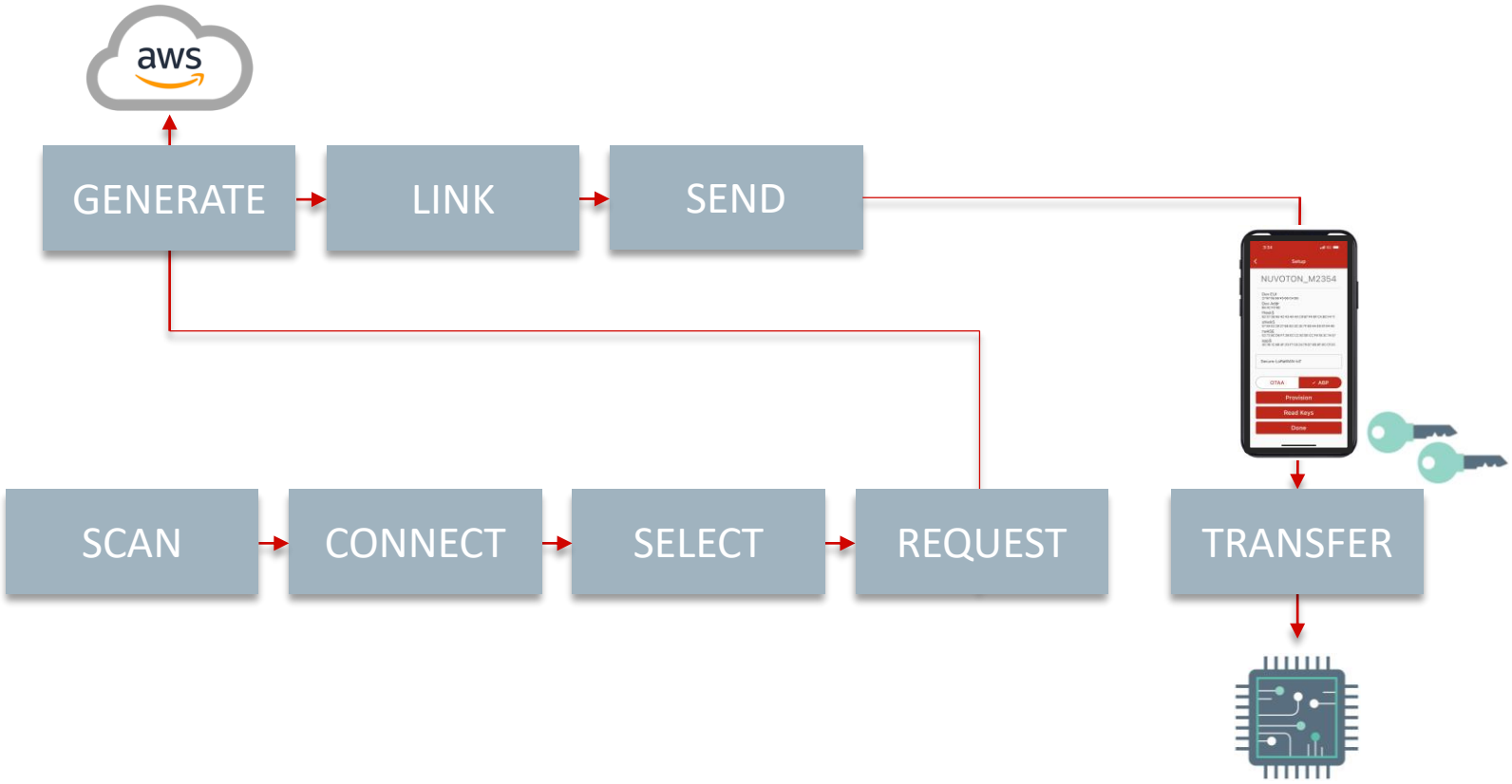
The Out-of-Box Experience

Then the server will send the provisioning Keys back to the Mobile App



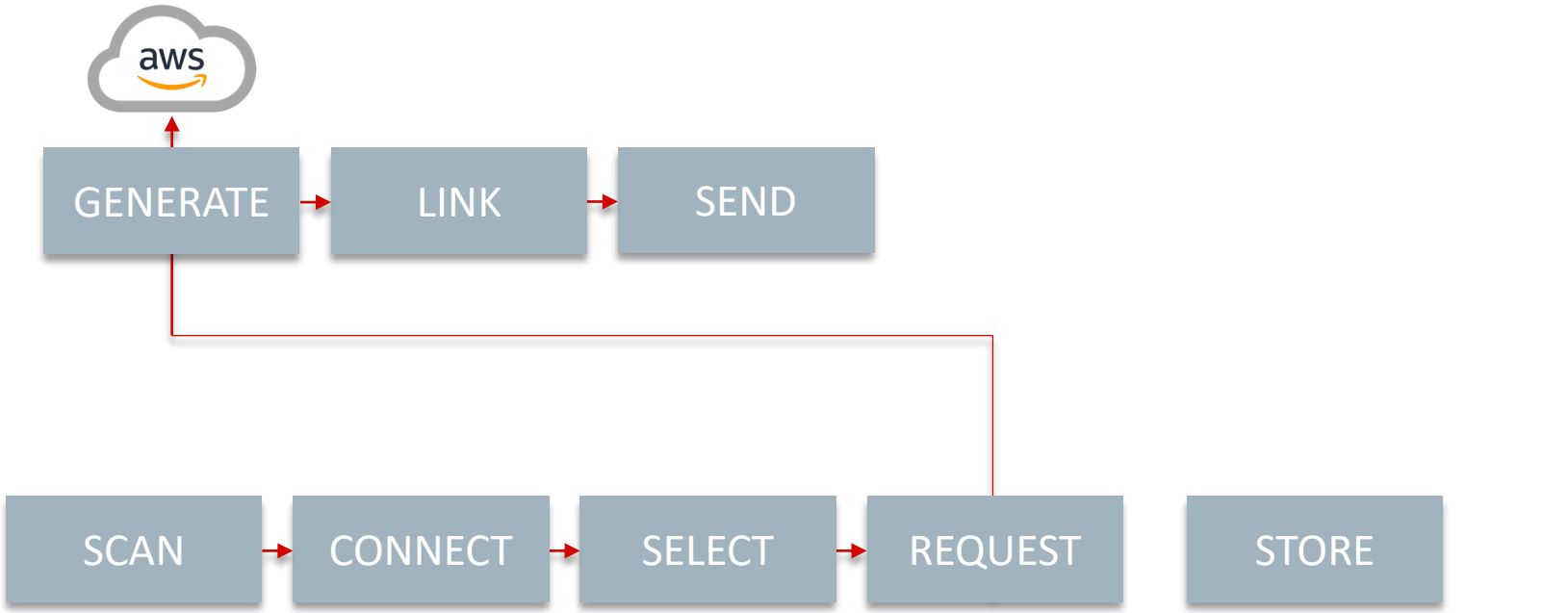
The Out-of-Box Experience

Then the App will transfer the provisioning Keys over BLE to the Device



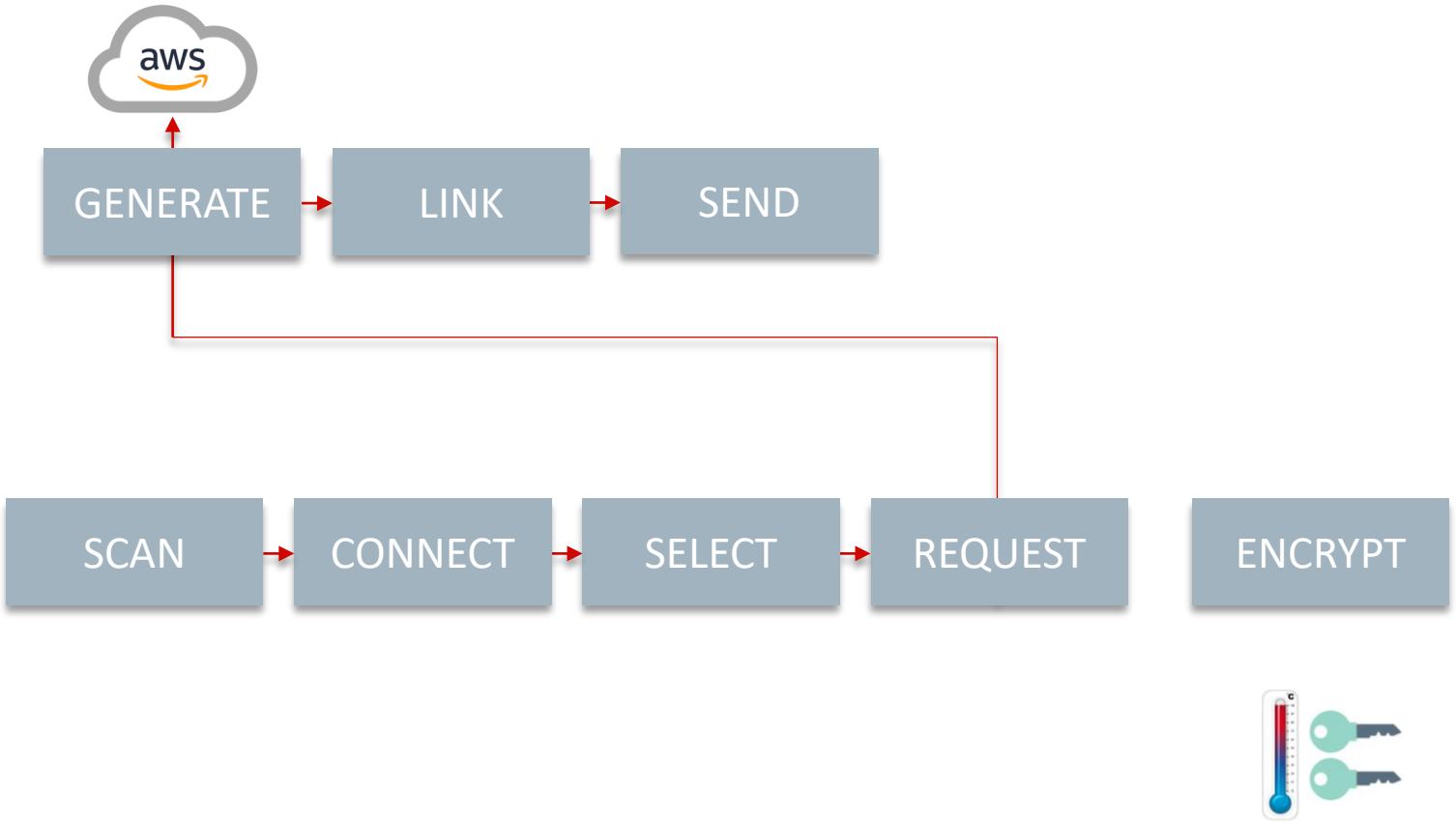
The Out-of-Box Experience

The Device will leverage KeyStore to store the Keys



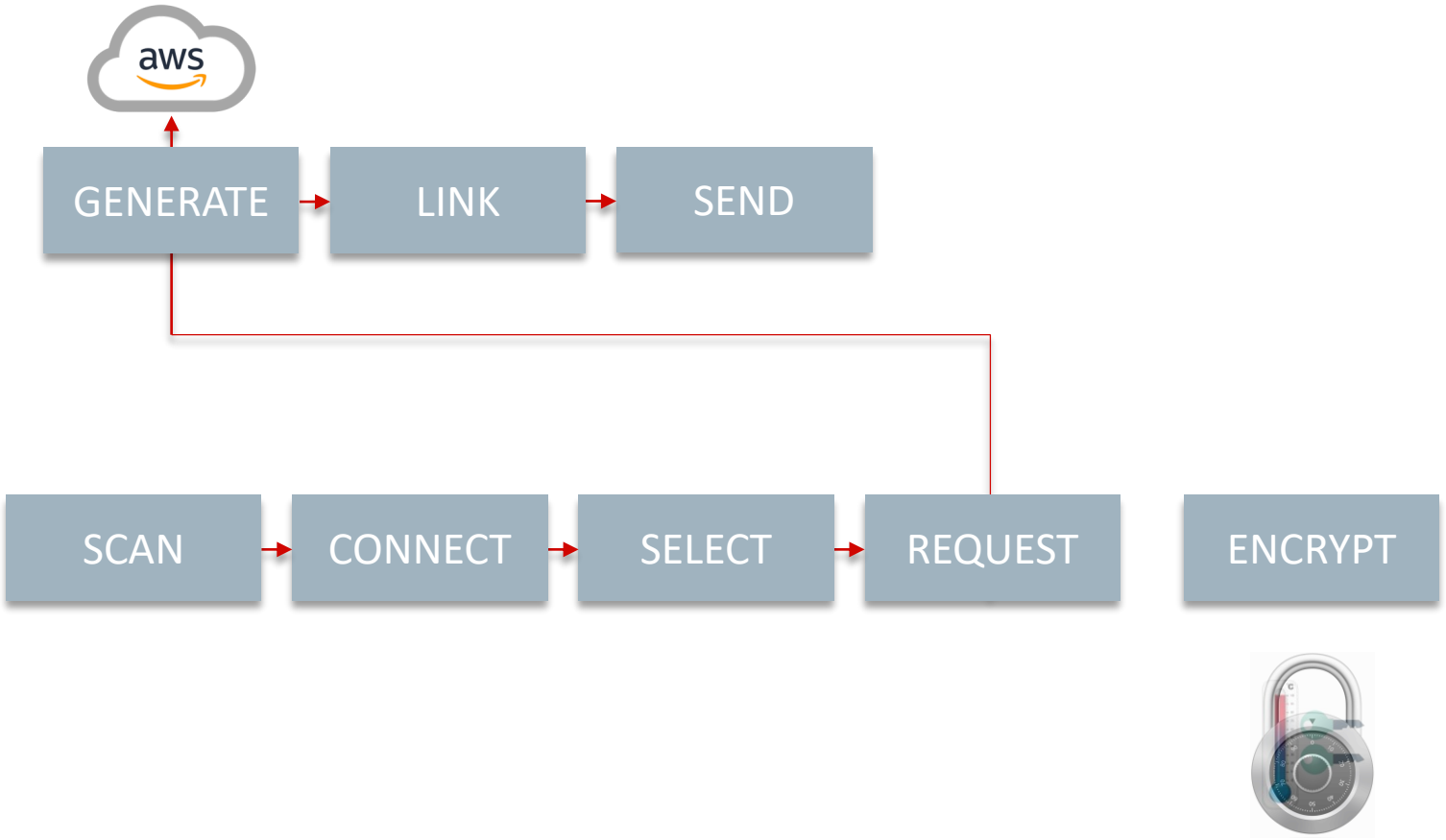
The Out-of-Box Experience

Then the LoRa MAC will leverage the M2354 Crypto Accelerator



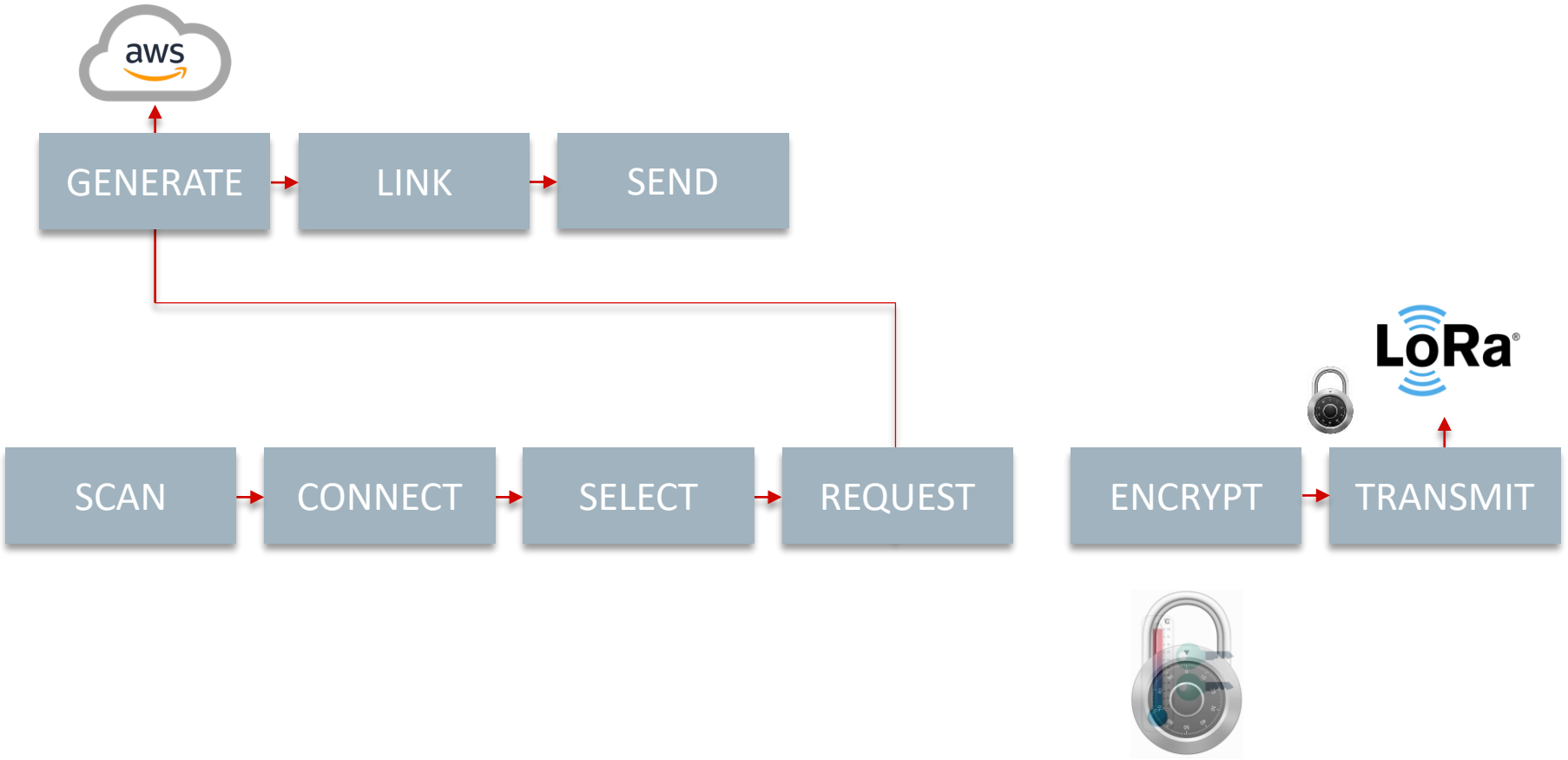
The Out-of-Box Experience

To encrypt the sensor data with the App Key and then encrypt with the Network Key



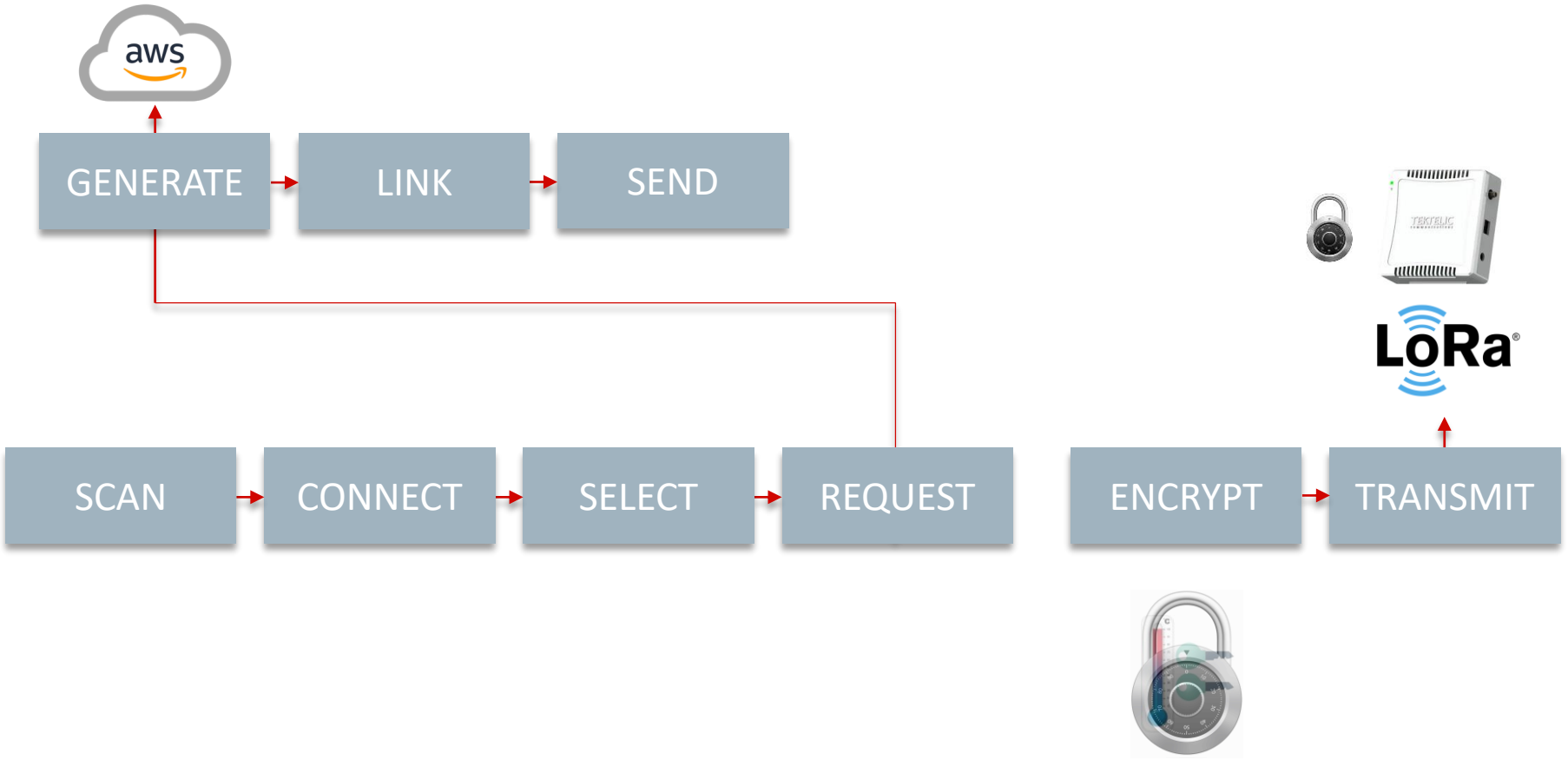
The Out-of-Box Experience

And then transmit the packet over LoRaWAN radio



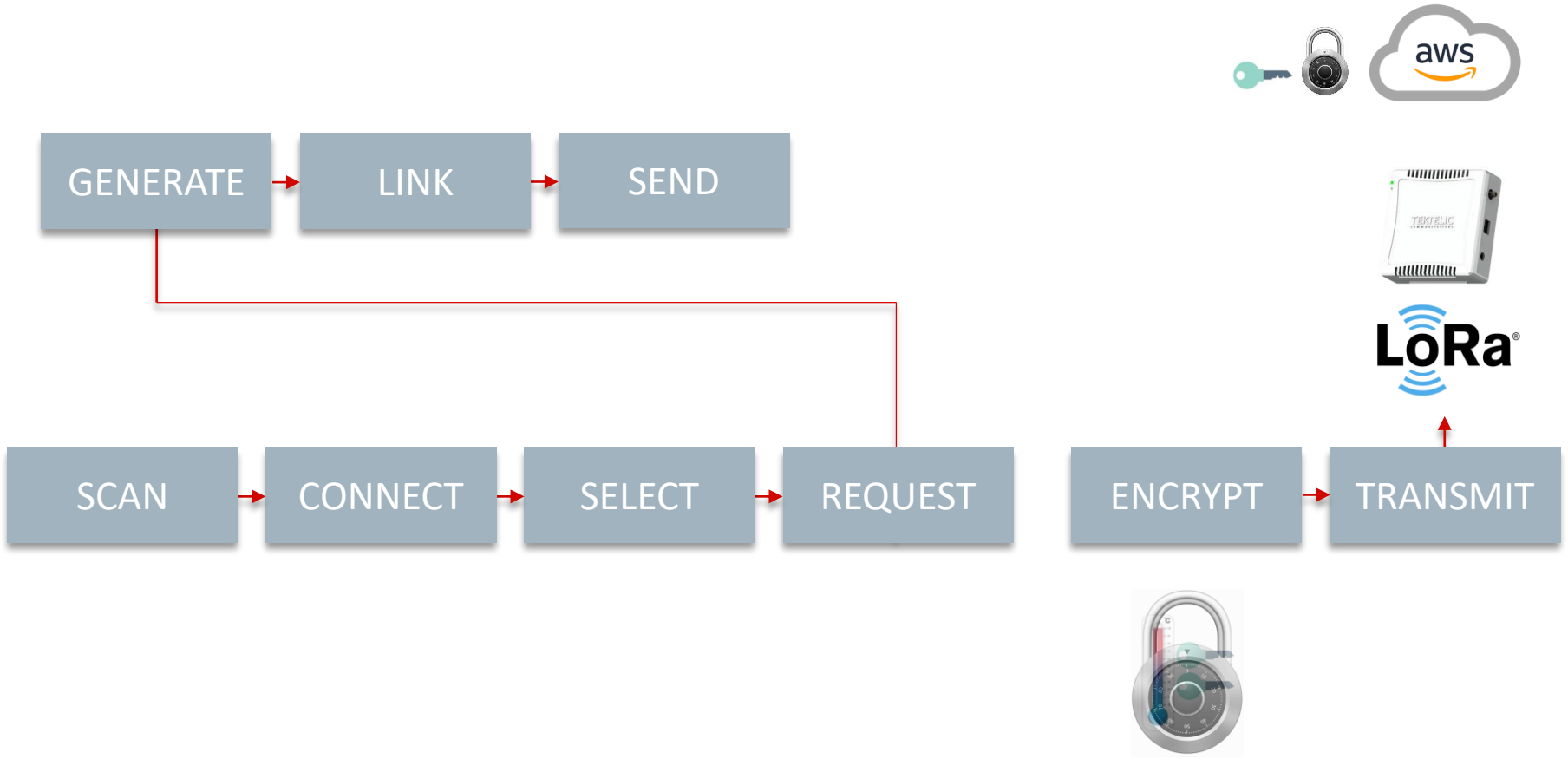
The Out-of-Box Experience

Then the LoRaWAN Gateway will capture the packet



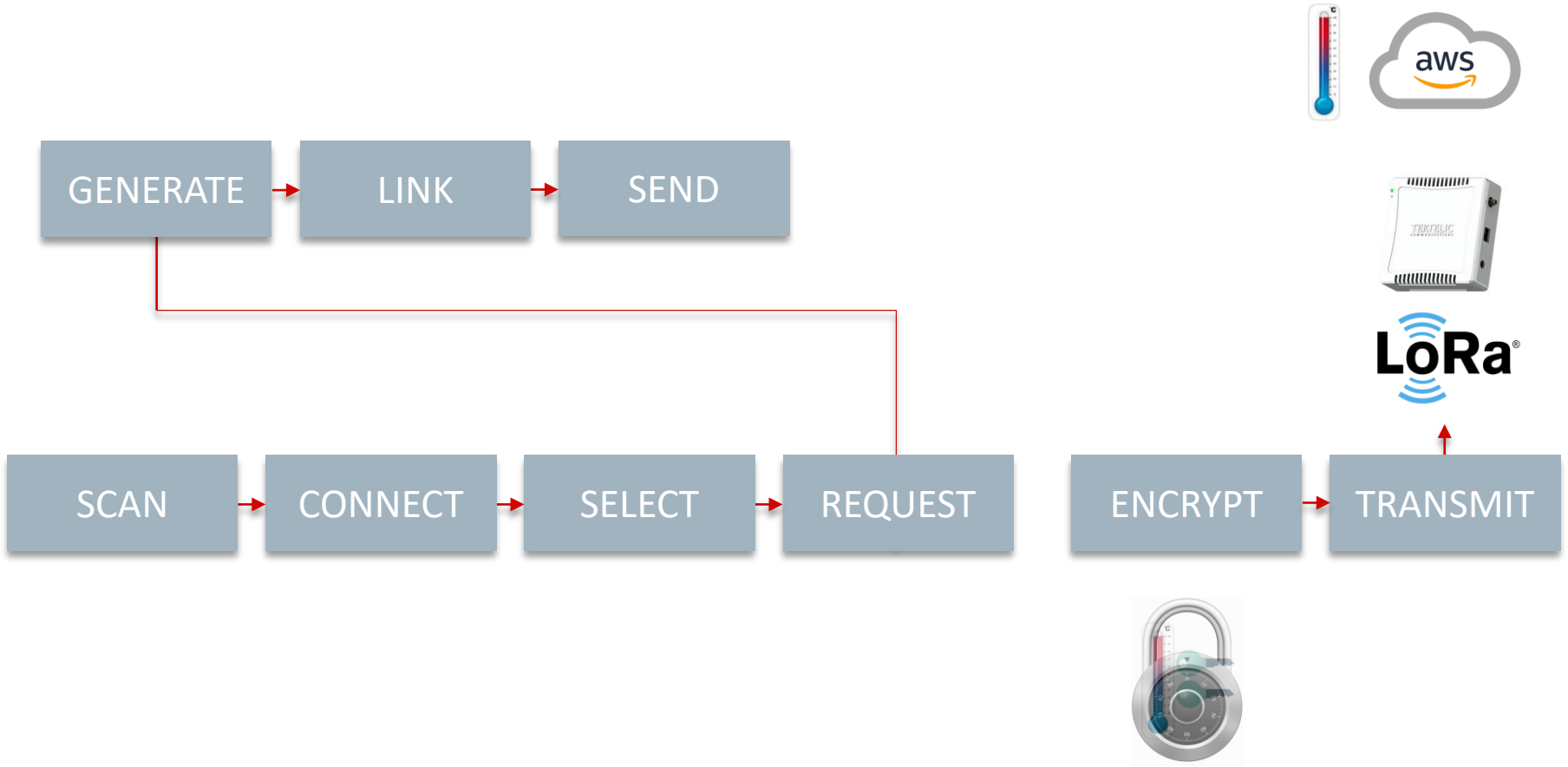
The Out-of-Box Experience

Then the AWS IoT for LoRaWAN server will decrypt the packet with the Network Key



The Out-of-Box Experience

And parcel the packet to the appropriate applications

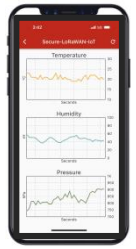


The Out-of-Box Experience

The Application can now use the Application Key to decrypt and use the data

The Out-of-Box Experience

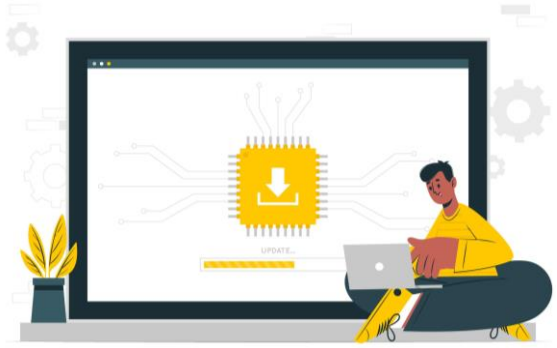
In this case:
Temperature,
Humidity,
Pressure



The Out-of-Box Experience

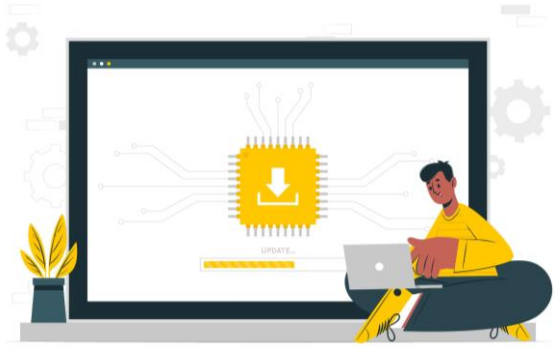
Ready to be integrated into End User's Application

Firmware



Ready to be integrated into End User's Application

Firmware



Remove Barrier to Entry

Improve Time to Market

Reduce Total Cost of Ownership

A Global Provisioning Partner

ECOSYSTEM

- Silicon Device Programming
- IoT Security Deployment As-a-Service

- Deliver secure and efficient systems to deploy firmware, data and secrets into IoT and automotive devices in high volume electronics manufacturing

Peace of Mind for IoT embedded designers

Peace of Mind for IoT embedded designers

Data Security

Protection of Core Assets:

IP
Customer Data
Acquired Knowledge

Peace of Mind for IoT embedded designers

Data Security

Protection of Core Assets:

IP
Customer Data
Acquired Knowledge

Operational Security

Uninterrupted
Business Operations

Peace of Mind for IoT embedded designers

Data Security	Operational Security	Business Security
Protection of Core Assets: IP Customer Data Acquired Knowledge	Uninterrupted Business Operations	Brand Protection

Next Gen based on Cortex-M33 in Development

Image Source:

https://community.arm.com/arm-community-blogs/b/architectures-and-processors-blog/posts/five-key-features-of-the-arm-cortex-m33-processor

Security

With Enhanced Device and Solution Features

Joy of innovation

NUVOTON

谢谢

謝謝

Děkuji

Bedankt

Thank you

Kiitos

Merci

Danke

Grazie

ありがとう

감사합니다

Dziękujemy

Obrigado

Спасибо

Gracias

Teşekkür ederim

Cảm ơn