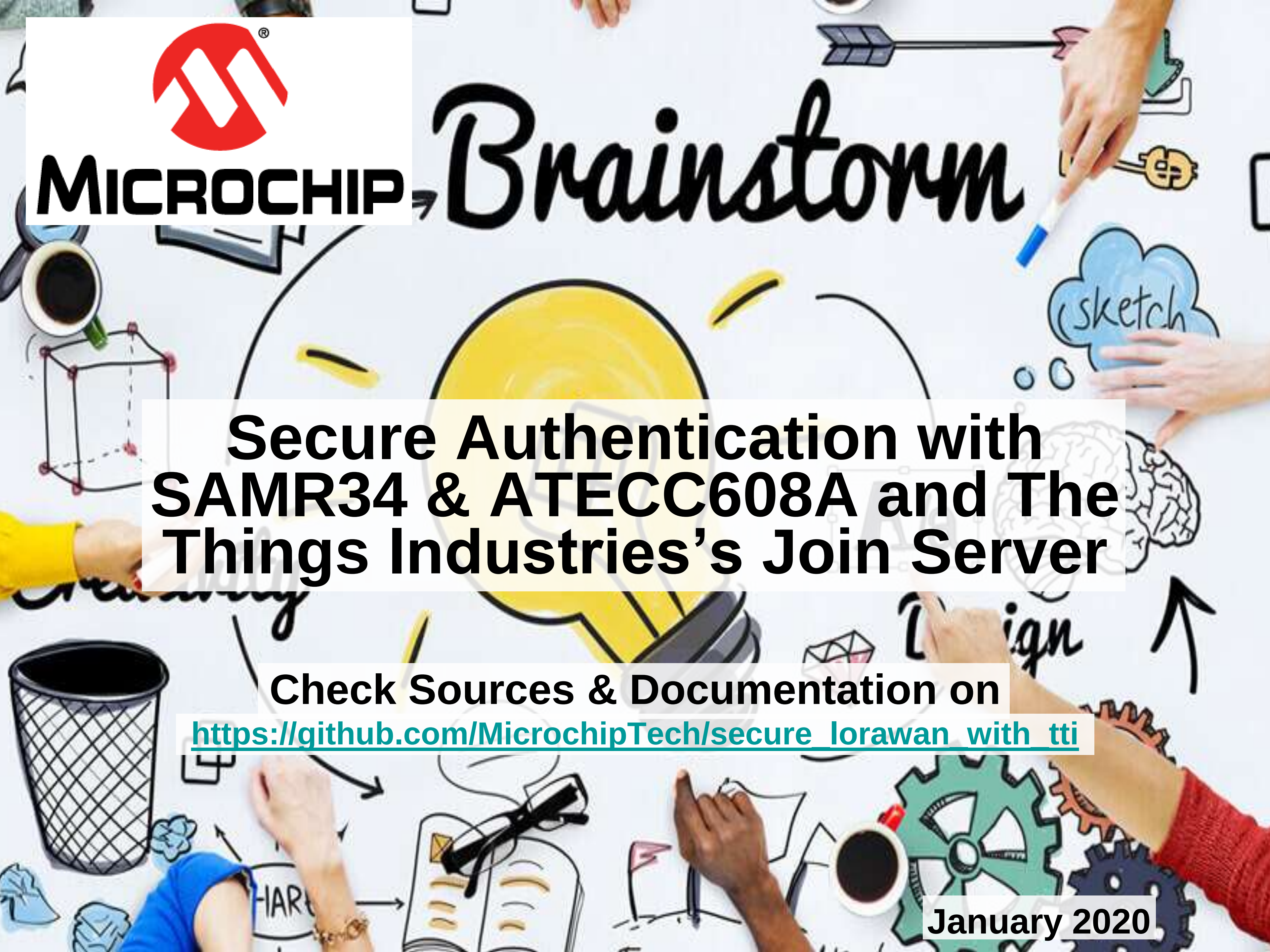
MICROCHIP



Secure Authentication with SAMR34 & ATECC608A and The Things Industries's Join Server

Check Sources & Documentation on

https://github.com/MicrochipTech/secure_lorawan_with_tti

January 2020

ACME Freezer Company

Specialist in Commercial Food Industry

Our restaurant clients are complaining of food loss from doors left open.

Let’s wirelessly monitor internal temperature & door position

Yes! A LoRaWAN device is battery operated & penetrates deep into buildings.

Jeroen, our « Creative » R&D designer

Me

The Team in charge of solving this challenge today

Gregory, Project Manager which will lead this session

Johan, our « Cool » Product Architect

Agenda

```
Start provisioning!
Enter DevEui [hex 8-bytes/16-char]: 1122334455667701
Enter JoinEui [hex 8-bytes/16-char]: 1122334455667788
Enter AppKey [hex 16-bytes/32-char]: 11223344556677881122334455667788

DevEui: 1122334455667701
JoinEui: 1122334455667788
AppKey: 11223344556677881122334455667788

1. Confirm the provisioning
2. Modify the provisioning
```

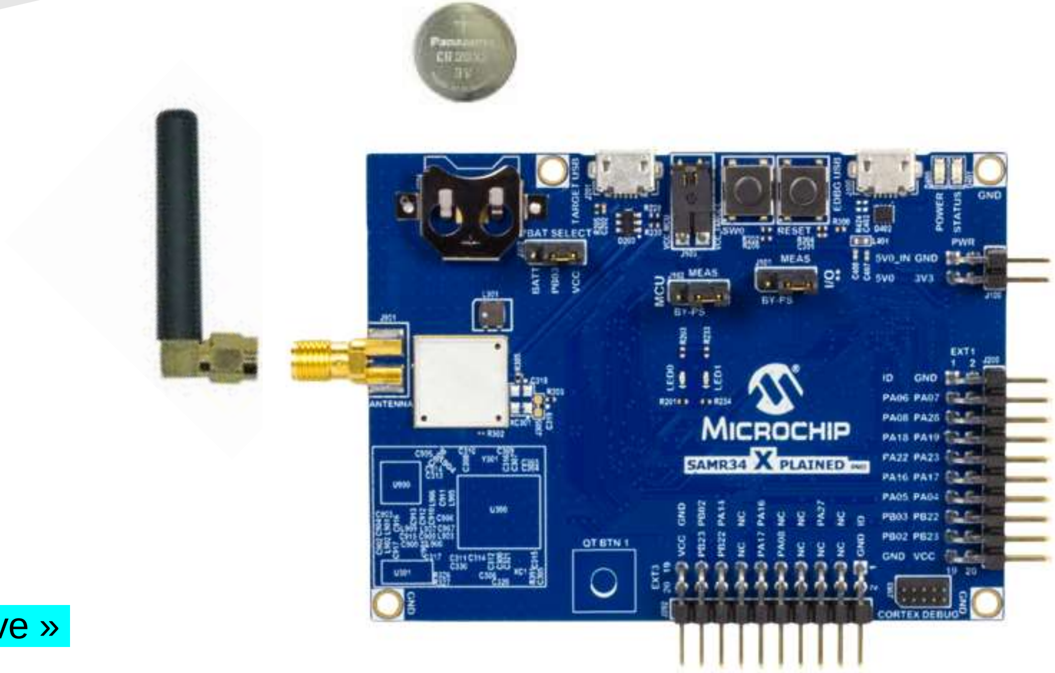
Me, a happy developper
My task : ensure that our product gets ready for production

- **Getting started with our project (10min)**
- **Lab 1 : Let’s connect our device to TTI Server (15min)**
- **What we learnt, how can we make things better (10min)**
- **Lab 2 : let’s make our solution more robust and secure (15min)**
- **Take Away (5min)**

« We have the Solution »

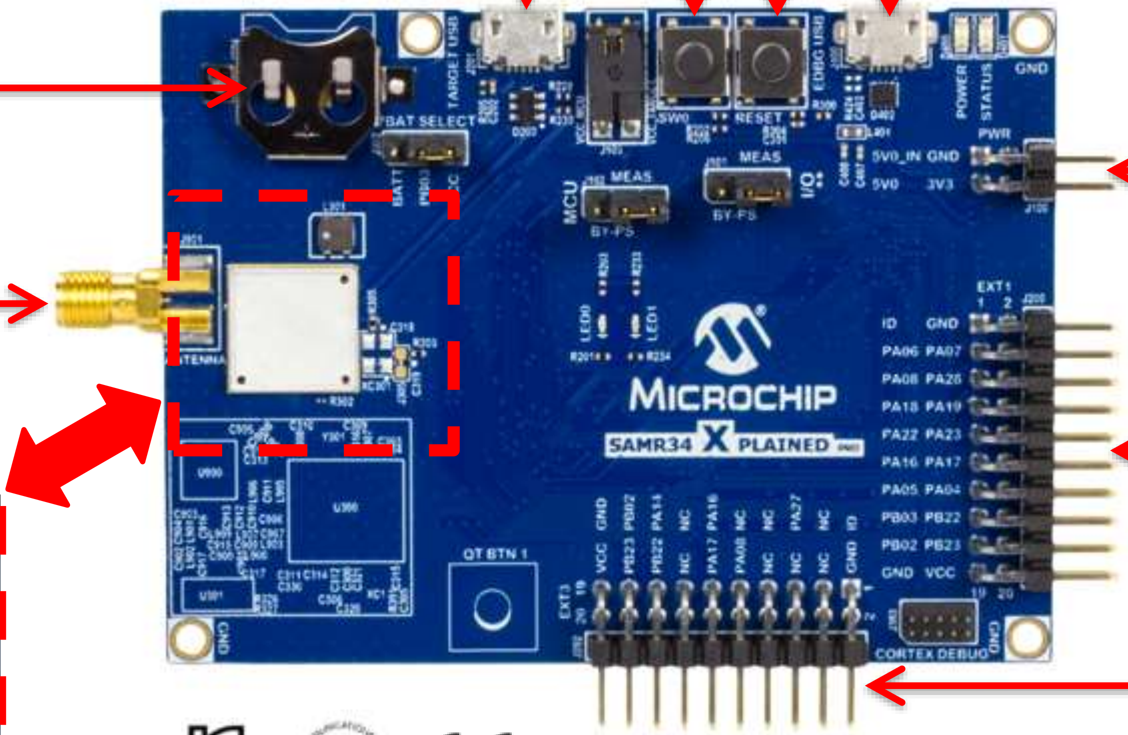
Prototype is now completed and ready to go based on SAMR34 LoRa MCU from Microchip and The Things Network Infrastructure. 10 sensors have been manufactured and validated by customers. We have a solution.

Jeroen, our « Creative »
R&D designer



LPWAN Design made *Easy*

Ordering Information : DM320111



Target USB

User Button

Reset Button

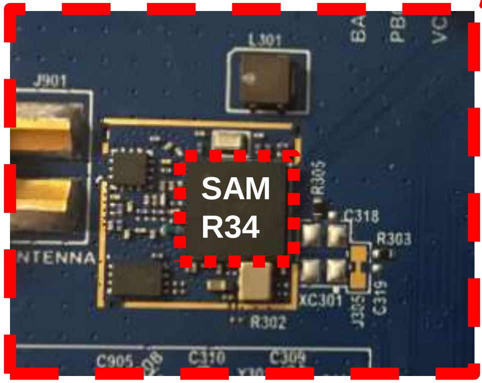
Debug USB

Coin-cell battery

External Antenna Connector

Power Header

Extension Header



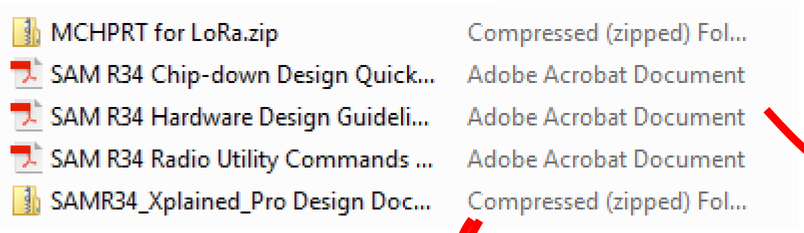
Fully **Certified development tool**

Reuse and copy/paste it onto your design

LPWAN Design made *Easy*

⌄ Design Guides

SAM R34 Chip-down Design Package



MCHPRT for LoRa.zip	Compressed (zipped) Fol...
SAM R34 Chip-down Design Quick...	Adobe Acrobat Document
SAM R34 Hardware Design Guideli...	Adobe Acrobat Document
SAM R34 Radio Utility Commands ...	Adobe Acrobat Document
SAMR34_Xplained_Pro Design Doc...	Compressed (zipped) Fol...

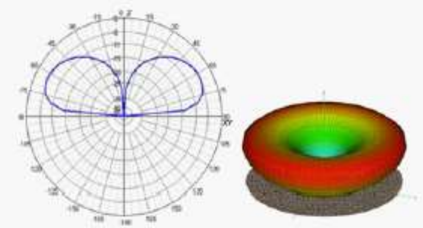
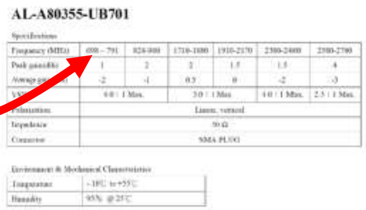


Figure 3-23. Example of an External Antenna



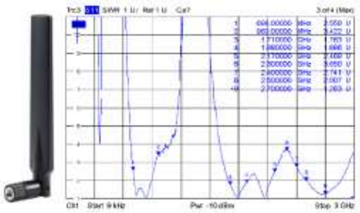
AL-A80355-UB701

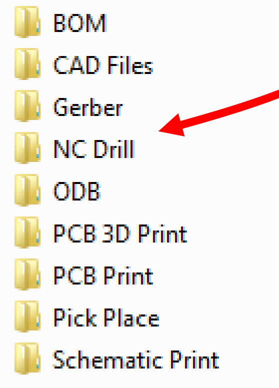
Specifications

Frequency (MHz)	698 – 791	824-960	1710-1880	1910-2170	2300-2400	2500-2700
Peak gain(dBi)	1	2	2	1.5	1.5	4
Average gain(dB)	-2	-1	0.5	0	-2	-3
VSWR	4.0 : 1 Max.		3.0 : 1 Max		4.0 : 1 Max.	2.5 : 1 Max.
Polarization	Linear, vertical					
Impedance	50 Ω					
Connector	SMA PLUG					

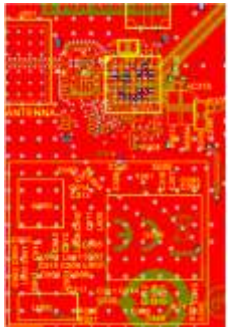
Environment & Mechanical Characteristics

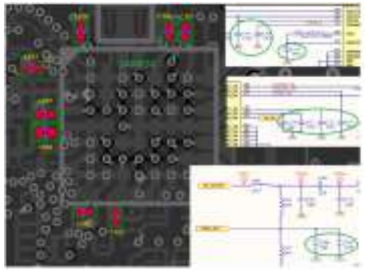
Temperature	-10℃ to +55℃
Humidity	95% @ 25℃

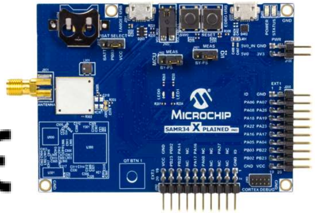


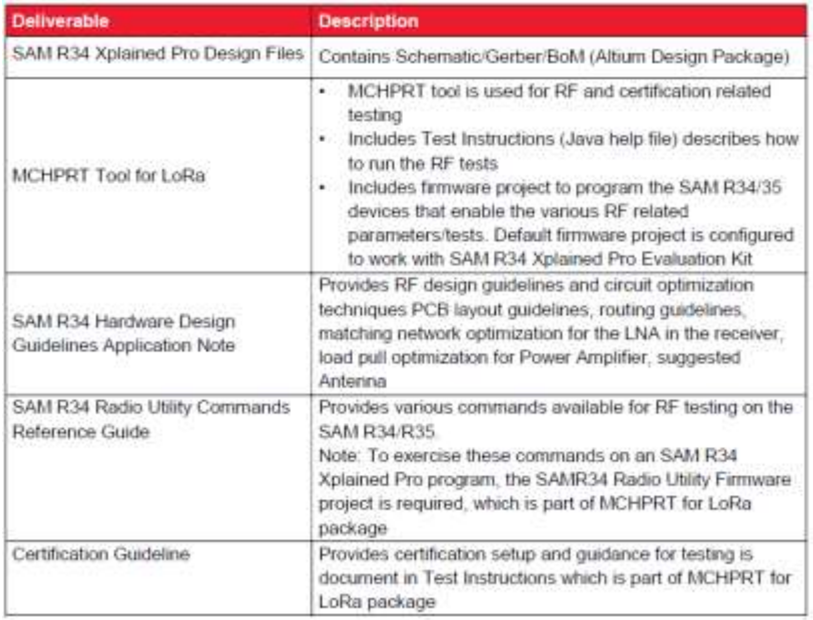


- BOM
- CAD Files
- Gerber
- NC Drill
- ODB
- PCB 3D Print
- PCB Print
- Pick Place
- Schematic Print









Deliverable	Description
SAM R34 Xplained Pro Design Files	Contains Schematic/Gerber/BoM (Altium Design Package)
MCHPRT Tool for LoRa	• MCHPRT tool is used for RF and certification related testing • Includes Test Instructions (Java help file) describes how to run the RF tests • Includes firmware project to program the SAM R34/35 devices that enable the various RF related parameters/tests. Default firmware project is configured to work with SAM R34 Xplained Pro Evaluation Kit
SAM R34 Hardware Design Guidelines Application Note	Provides RF design guidelines and circuit optimization techniques PCB layout guidelines, routing guidelines, matching network optimization for the LNA in the receiver, load pull optimization for Power Amplifier, suggested Antenna
SAM R34 Radio Utility Commands Reference Guide	Provides various commands available for RF testing on the SAM R34/R35 Note: To exercise these commands on an SAM R34 Xplained Pro program, the SAMR34 Radio Utility Firmware project is required, which is part of MCHPRT for LoRa package
Certification Guideline	Provides certification setup and guidance for testing is document in Test Instructions which is part of MCHPRT for LoRa package

LPWAN Design made *Easy*

- **State of the art LoraWAN Stack (ASF)**
  - Developed, maintained and supported by Microchip

- **Firmware matters. And we have it !**
  - Many firmware resources to learn from
  - Getting Started Package from Microchip
    - ww1.microchip.com/downloads/en/DeviceDoc/Quick%20Start%20Guides%20for%20SAMR34%20Applications%20in%20ASF3.zip
  - Microchip Github
    - https://github.com/MicrochipTech
  - TTN Community Forum
    - www.thethingsnetwork.org/u/GDemont

SAM R34/R35 Low Power LoRa® Sub-GHz System-in-Package Family

Industry's Lowest Power LoRa SiP for Long Range, Low Power Designs

[illegible]

[illegible]

Ultra-low power SAM R34 SiP devices
Comprehensive evaluation kit
Certified chip-down design package
Proven Microchip stack and software
Technical support for every phase

Connecting the Microchip ATSAMR34 Xplained Pro Kit [illegible] LoRaWAN to The Things Network

Upgrading LoRaWAN Application by adding Secure Communication and Secure Key Provisioning onto Microchip ATSAMR34 Xplained Pro Kit

Upgrading LoRaWAN Application by adding LoRa Peer-to-Peer Link onto Microchip ATSAMR34 Xplained Pro Kit

Upgrading LoRaWAN Application by adding WiFi [illegible] to Cloud [illegible] onto Microchip ATSAMR34 Xplained Pro Kit

UPGRADING LORAWAN APPLICATION BY ADDING BLE [illegible] TO PROVISIONING & LOCAL DEBUGGING ONTO MICROCHIP ATSAMR34 XPLAINED PRO KIT

- **Security matters with LoraWAN. And we have it !**
  - Trust&GO LoRa® Secure Authentication with the ATECC608A Secure Element
    - Pre-provisioned secure element for LoRaWAN
    - Comes with the authentication keys of The Things Industries (TTI) or Actility join servers
  - Get started in no time with our solution on Github
    - https://github.com/MicrochipTech/atsamr34_ecc608a_tti
    - https://github.com/MicrochipTech/atsamr34_ecc608a_actility

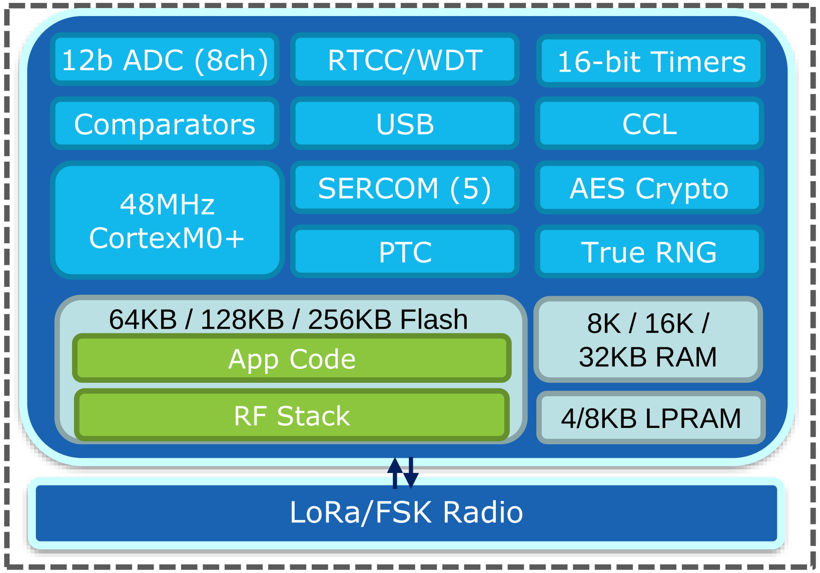
ATECC608A-TNGLORA

www.microchip.com/ATECC608A-TNGLORA

www.microchip.com/design-centers/wireless-connectivity/low-power-wide-area-networks/lora-technology/sam-r34-r35

SAMR34 / R35
Standalone LoRa MCU

- **Highly Integrated MCU with Lora Radio**
  - Cortex M0+ MCU at 48MHz
  - 64 / 128 / 256KB Flash
  - Backup RAM retention for frame counters
  - Ultra Low Power Consumption
  - Hardware AES crypto accelerators
  - True Random Number Generator
  - 6 Timer/Counters, RTC and WDT
  - 5 SERCOMs (USART, I2C, SPI , LIN)
  - Full Speed USB
  - High performance ADC and analog peripherals for sensor nodes
  - 27 Programmable I/O Pins
  - RF Features : Lora Transceiver
    - 169, 433, 780, 868 & 915MHz band support
    - Lora, GFSK, GMSK, and OOK



12b ADC (8ch)
RTCC/WDT
16-bit Timers
Comparators
USB
CCL
48MHz CortexM0+
SERCOM (5)
AES Crypto
PTC
True RNG
64KB / 128KB / 256KB Flash
App Code
RF Stack
8K / 16K / 32KB RAM
4/8KB LPRAM
LoRa/FSK Radio

Part Number	Flash	RAM	LP-RAM	USB
ATSAMR34J16BT-I/7JX	64 KB	8 KB	4 KB	Yes
ATSAMR34J17BT-I/7JX	128 KB	16 KB	8 KB	Yes
ATSAMR34J18BT-I/7JX	256 KB	32 KB	8 KB	Yes
ATSAMR35J16BT-I/7JX	64 KB	8 KB	4 KB	No
ATSAMR35J17BT-I/7JX	128 KB	16 KB	8 KB	No
ATSAMR35J18BT-I/7JX	256 KB	32 KB	8 KB	No

The SAMR34 and ECC608 are fully available and in production Now ! With a fully certified reference design, HW & FW. Risk free & short Time to Market. Good choice Jeroen

Johan, our « Cool » Product Architect

www.microchip.com/design-centers/wireless-connectivity/low-power-wide-area-networks/lora-technology/sam-r34-r35

LoRaWan Cloud Options

- **The Things Network Solution**
  - An Open and free-to-use community network
  - A Decentralized, Open and Crowdsourcing IoT data network Owned and Operated by its Users
  - Many resources and comprehensive LoRaWAN network coverage allowing fast and easy protoyping. Validate a concept in no time!
  - TTN V2 Server supports LoRaWAN™ 1.0.2 specs and Class A only

www.thethingsnetwork.org

- **The Things Industries Solutions**
  - A comprehensive LoRaWAN solution with enterprise grade stack that fits requirements for security, scalability and robustness. TTI brings all the resources required to build an IoT infrastructure
  - End-to-end LoRaWAN security with TTI Join Server and Microchip ATECC608A-TNGLORA Secure Element
  - TTI v3 Server supports:
    - LoRaWAN™ 1.0, 1.0.1, 1.0.2, 1.0.3 and 1.1 natively, 1.0.4 on roadmap
    - LoRaWAN™ Class A, C (now), B (on roadmap)
    - Peering, Multi-tenancy, LoRaWAN™ Multicast
    - Firmware Update Over the Air (FUOTA)
  - Proposed Services
    - Saas, Private Cloud (run the network server in customer's cloud), On-Site (rounting services run on customer's premise or on the gateway itself)
    - More info : www.youtube.com/watch?v=X6nNXy_VlYE

www.thethingsindustries.com

Feedbacks from Management

Hold on, guys !
TTI makes sense to scale our deployment. So let’s use it
<u>But</u> why security for a simple temperature sensor ???

Secure Element

What we have works ! Why changing ?

This brings extra hardware so extra cost

More complexity in R&D so longer time to market and extra cost

We will become tied-up to TTI, and this forever. No way out !!!

More complexity in Production so again longer time to market and extra cost

Clayton, our Grumpy Boss

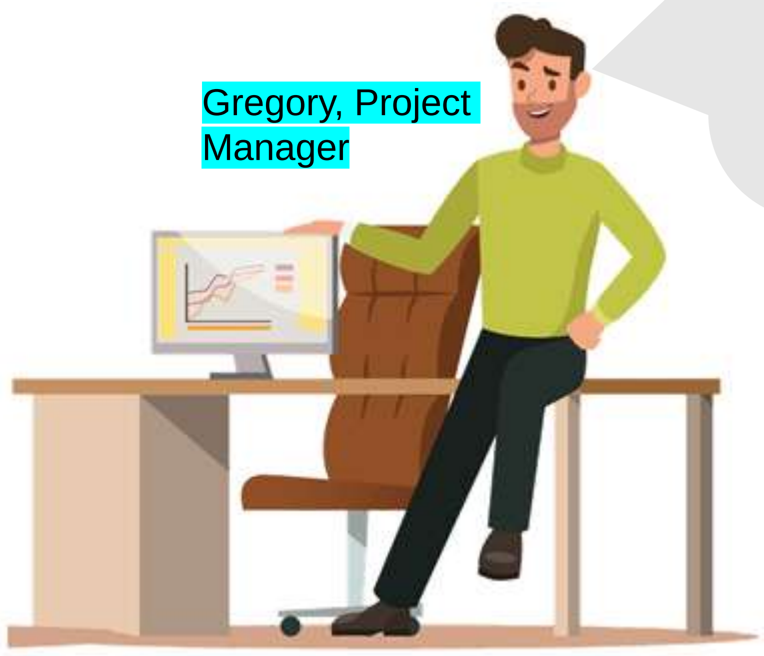
Lab 1

Ok guys, let’s follow the guidelines from Clayton :

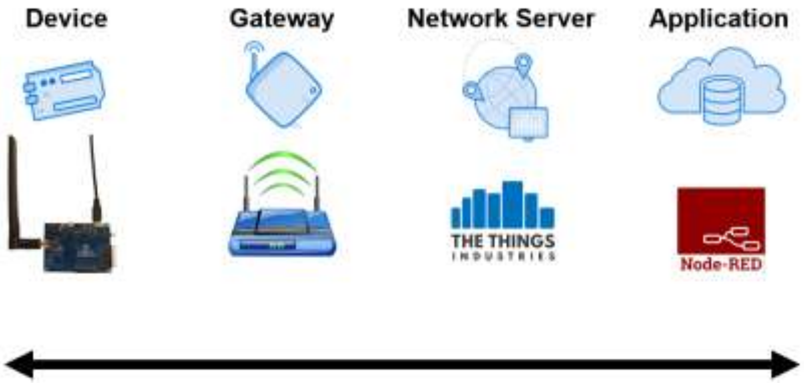
1) Set-up your TTI session on their web portal (Console)

2) Provision your Sensor (entered keys and name your device) so our device get connected to TTI Network Server

3) Validate that every sensors in the field reports its temperature properly back to our Company dashboard



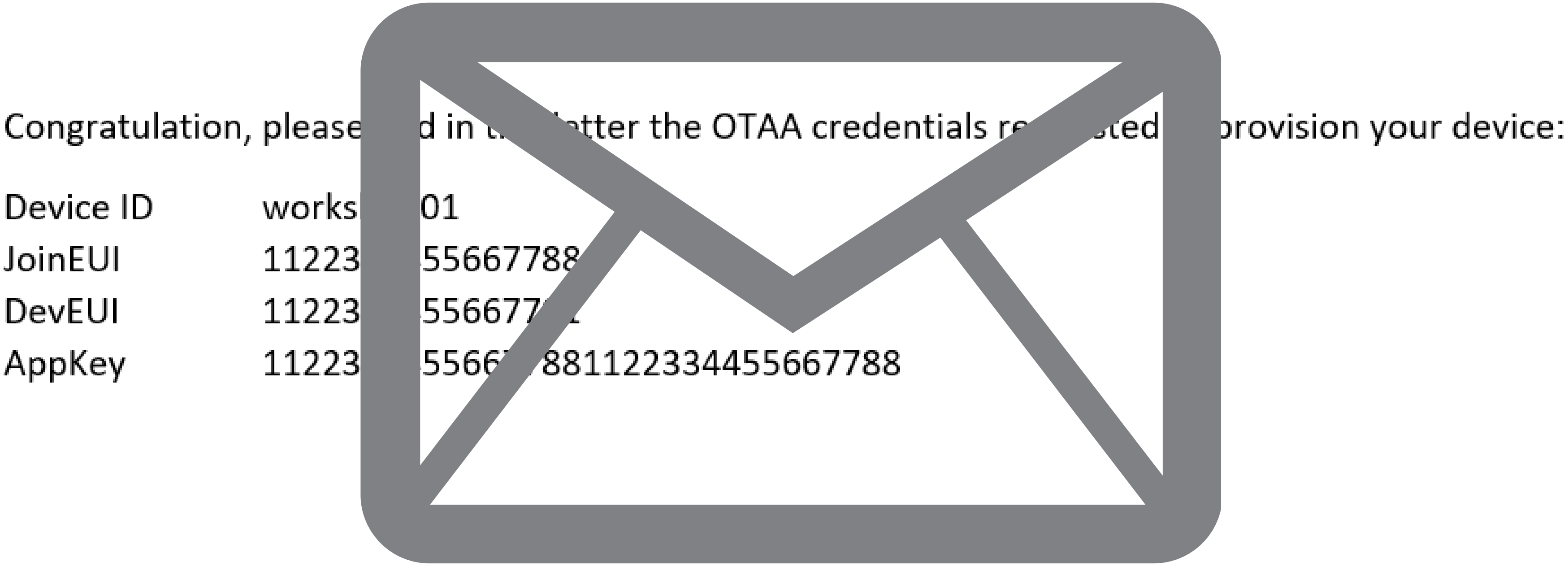
Gregory, Project Manager



Lab Material

- **The Things Industries Network Server Account**
- **A set of root keys for OTAA**
  - DevEUI
  - AppEui/JoinEUI
  - AppKey
- **A SAMR34 Xpro board pre-loaded with an ASF application specifically written for this workshop**
- **A micro-USB cable**
- **An RF antenna**

How we get Root Keys today



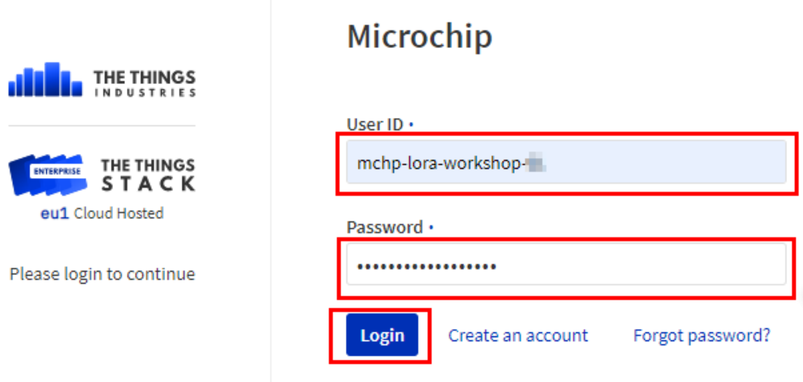
Congratulation, please d in t etter the OTAA credentials re sted provision your device:

Device ID	works 01
JoinEUI	11223 55667788
DevEUI	11223 556677
AppKey	11223 5566 8811223344556677 88

https://github.com/MicrochipTech/secure_lorawan_with_tti

TTI Network Server Login

- **Open the TTI Network Server Console: https://microchip.eu1.cloud.thethings.industries/console**
- **Login by using the TTI Credentials provided within the appendix sheet**



THE THINGS INDUSTRIES

ENTERPRISE THE THINGS STACK eu1 Cloud Hosted

Please login to continue

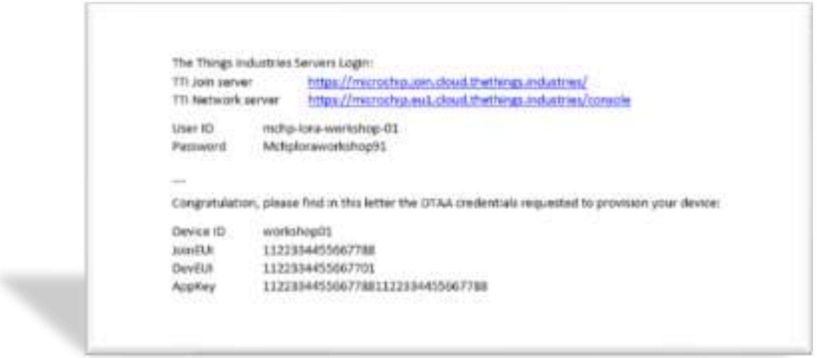
Microchip

User ID •

mchp-lora-workshop-[redacted]

Password •

••••••••••••••••••



The Things Industries Servers Login:

TTI Join server https://microchip.join.cloud.thethings.industries/

TTI Network server https://microchip.eu1.cloud.thethings.industries/console

User ID mchp-lora-workshop-01

Password Mchploraworkshop91

—

Congratulation, please find in this letter the OTAA credentials requested to provision your device:

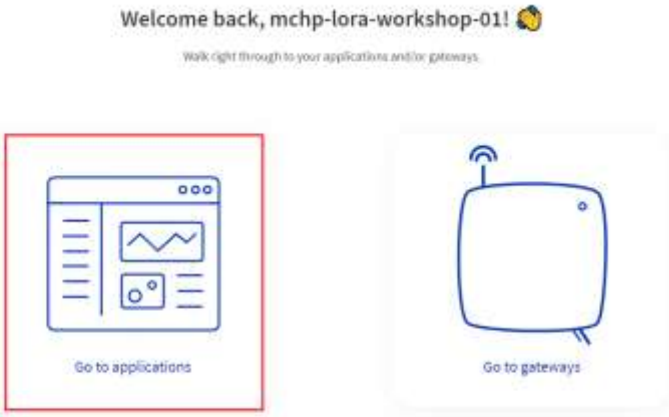
Device ID workshop01

JoinEUI 1122334455667788

DevEUI 1122334455667701

AppKey 11223344556677881122334455667788

- **Select Go to applications**

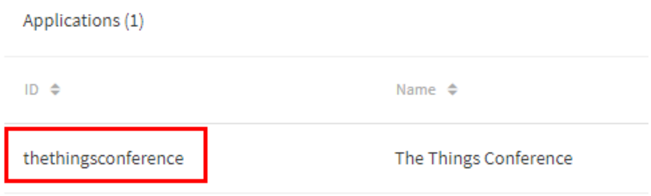


Welcome back, mchp-lora-workshop-01! 👋

Walk right through to your applications and/or gateways.

Select Application

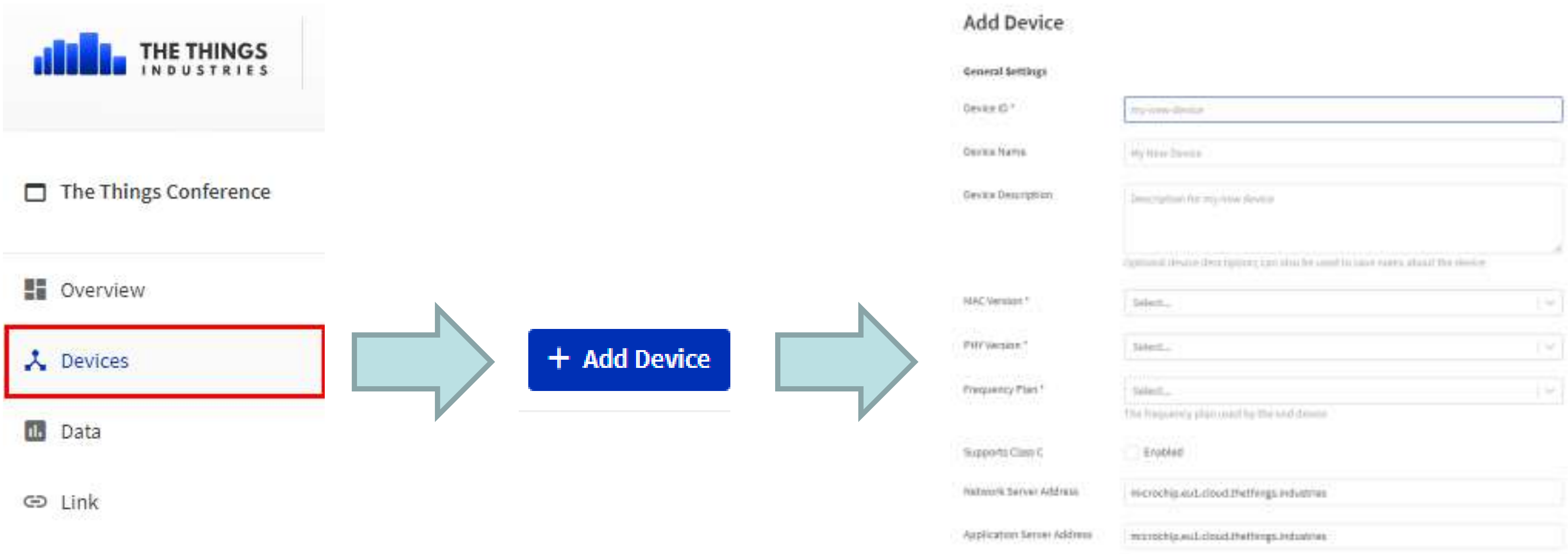
- **Select ‘thethingsconference’ application**



Applications (1)

ID	Name
thethingsconference	The Things Conference

- **Go to “Devices” in the left menu and click on “+ Add Device” to reach the end device registration page.**



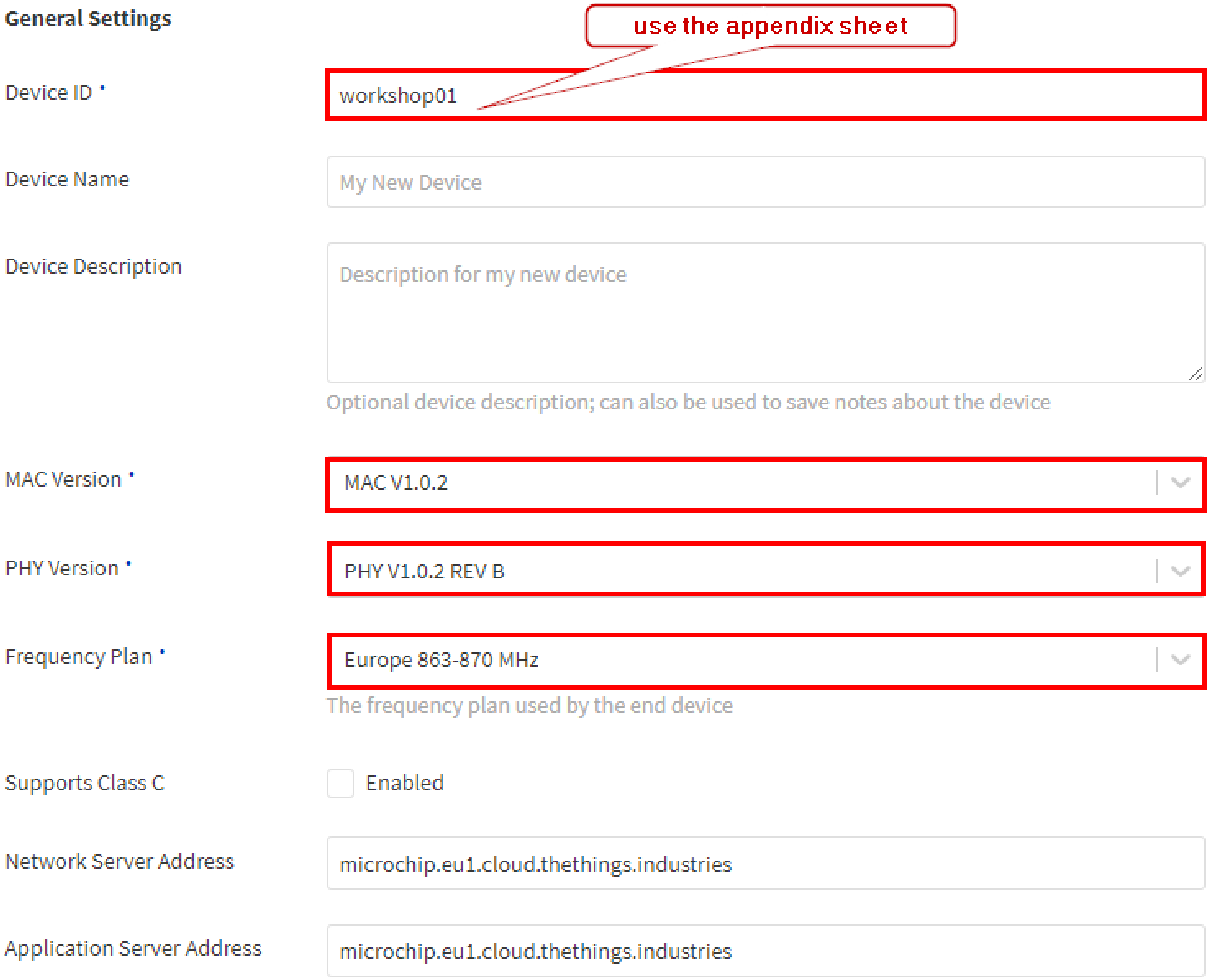
Add Device

General Settings

Device ID *	my-new-device
Device Name	My New Device
Device Description	Description for my new device Optional device description; can also be used to save notes about the device
MAC Version *	Select...
PHY Version *	Select...
Frequency Plan *	Select... The frequency plan used by the end device
Supports Class C	□ Enabled
Network Server Address	microchip.eu1.cloud.thethings.industries
Application Server Address	microchip.eu1.cloud.thethings.industries

Add Devices

- **General Settings**



use the appendix sheet

General Settings

Device ID * workshop01

Device Name My New Device

Device Description Description for my new device

Optional device description; can also be used to save notes about the device

MAC Version * MAC V1.0.2

PHY Version * PHY V1.0.2 REV B

Frequency Plan * Europe 863-870 MHz

The frequency plan used by the end device

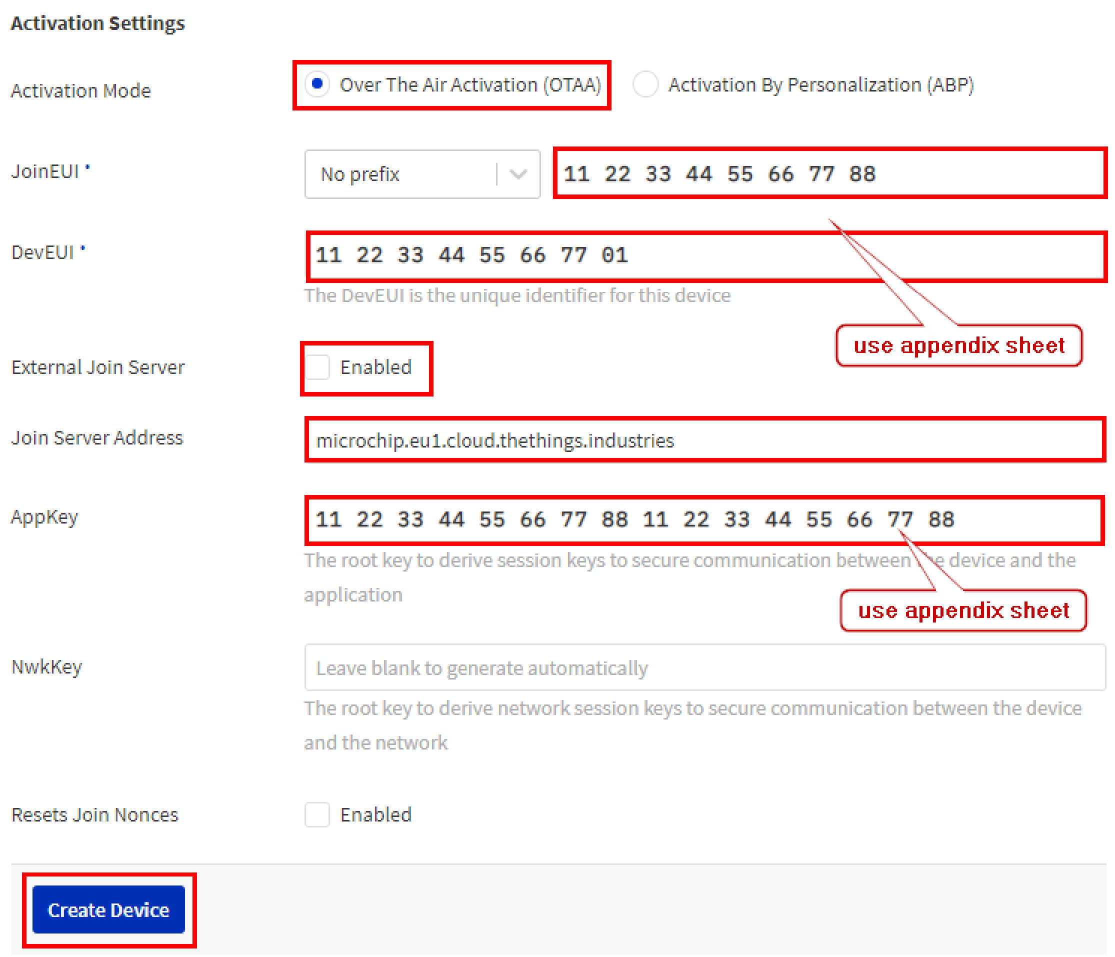
Supports Class C □ Enabled

Network Server Address microchip.eu1.cloud.thethings.industries

Application Server Address microchip.eu1.cloud.thethings.industries

Add Devices

- **Activation Settings**



Activation Settings

Activation Mode: ● Over The Air Activation (OTAA) ○ Activation By Personalization (ABP)

JoinEUI *: No prefix | 11 22 33 44 55 66 77 88

DevEUI *: 11 22 33 44 55 66 77 01

The DevEUI is the unique identifier for this device

use appendix sheet

External Join Server: □ Enabled

Join Server Address: microchip.eu1.cloud.thethings.industries

AppKey: 11 22 33 44 55 66 77 88 11 22 33 44 55 66 77 88

The root key to derive session keys to secure communication between the device and the application

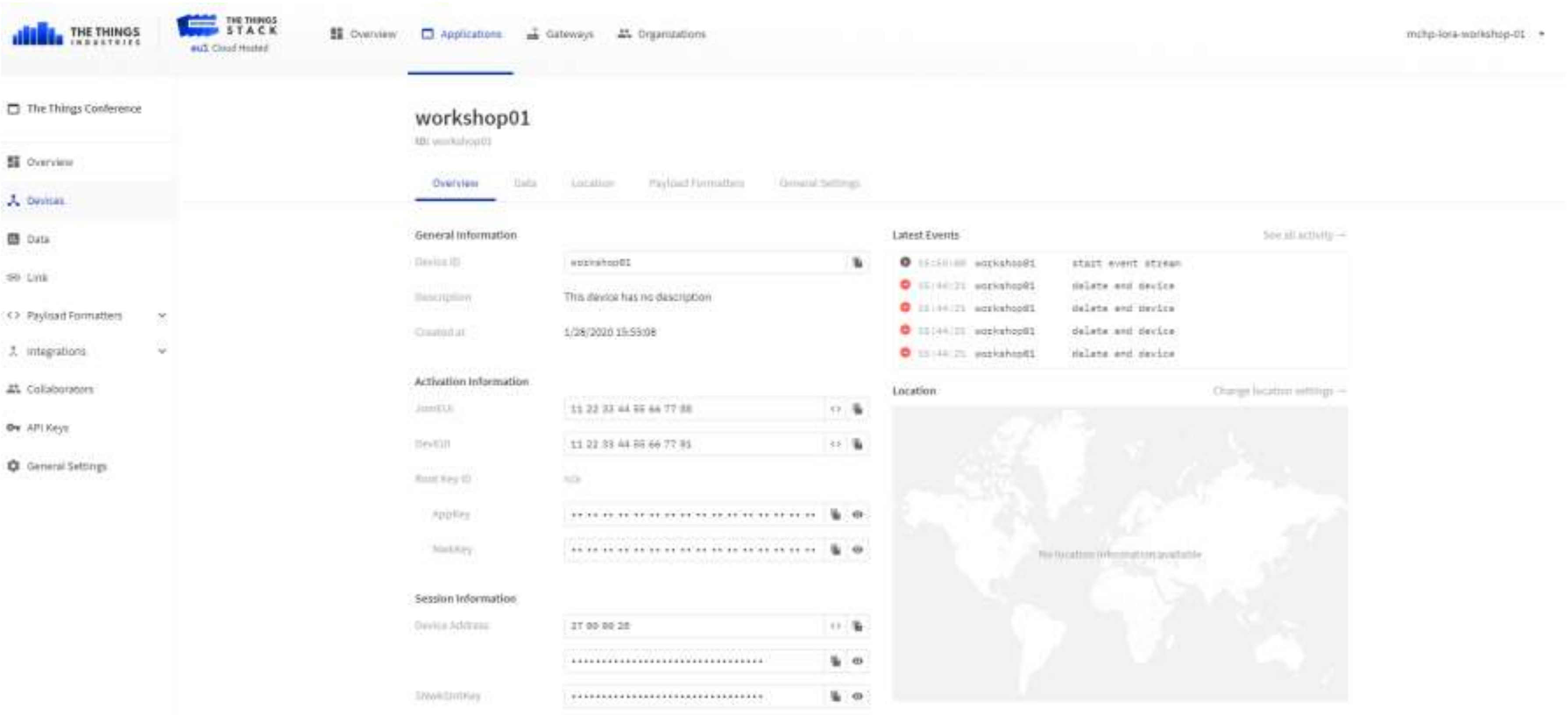
use appendix sheet

NwkKey: Leave blank to generate automatically

The root key to derive network session keys to secure communication between the device and the network

Resets Join Nonces: □ Enabled

Device Overview



workshop01

ID: workshop01

General Information

Device ID: workshop01

Description: This device has no description

Created at: 1/28/2020 15:59:08

Activation Information

JoinEUI: 11 22 33 44 55 66 77 88

DevEUI: 11 22 33 44 55 66 77 81

Root Key ID: n/a

AppKey: •• •• •• •• •• •• •• •• •• •• •• •• •• •• •• ••

NwkKey: •• •• •• •• •• •• •• •• •• •• •• •• •• •• •• ••

Session Information

Device Address: 27 00 00 28

••••••••••••••••••••••••••••••••

SNwkSIntKey: ••••••••••••••••••••••••••••••••

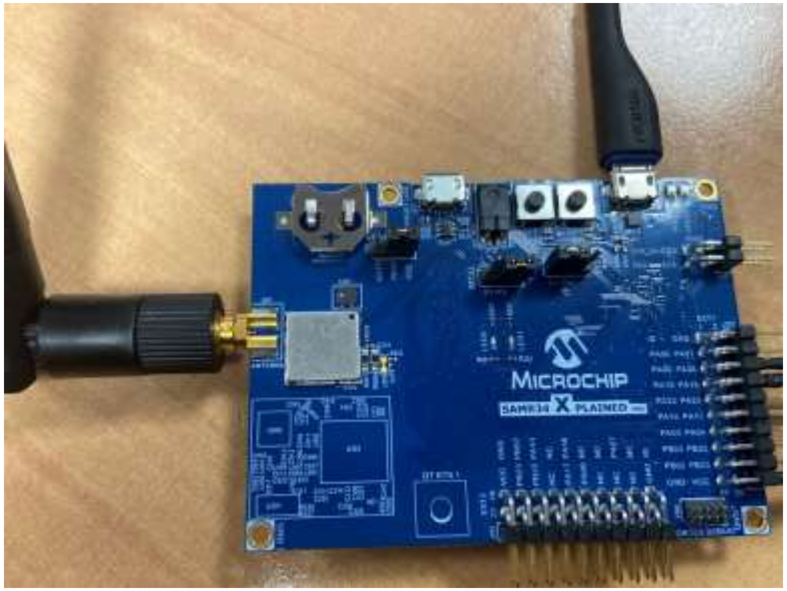
Latest Events

```
15:59:08  workshop01  start event stream
15:44:21  workshop01  delete end device
15:44:21  workshop01  delete end device
15:44:21  workshop01  delete end device
15:44:21  workshop01  delete end device
```

Location

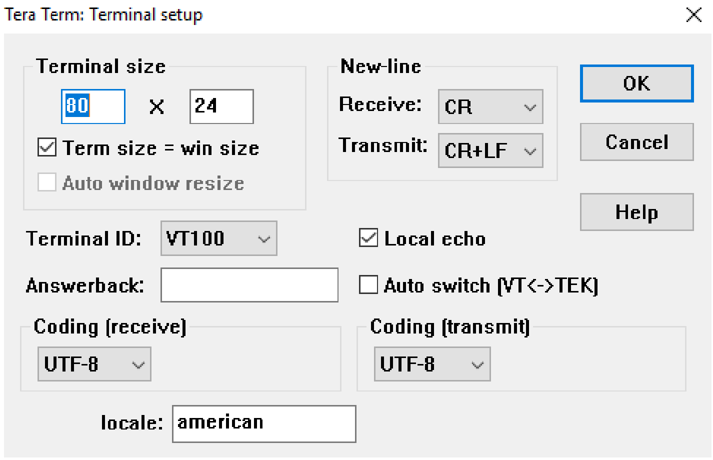
Hardware Setup

- **Plug the antenna and always make sure you have the antenna plugged to your SAMR34 Xpro board before powering it up**
- **Connect your SAMR34 Xpro board to the computer through the micro-USB cable. USB cable must be connected to the EDBG USB connector of the kit.**
- **Wait for USB driver installation and COM port mounting. The USB port powers the board and enables the user to communicate with the kit.**



Serial Console Setup

- Open Serial Console (e.g. TeraTerm)
- Configure Terminal setup
- Configure Serial port setup: COMxx 115200 bps / 8 / N / 1



Tera Term: Terminal setup

Terminal size

80 × 24

☑ Term size = win size

□ Auto window resize

New-line

Receive: CR

Transmit: CR+LF

Terminal ID: VT100

☑ Local echo

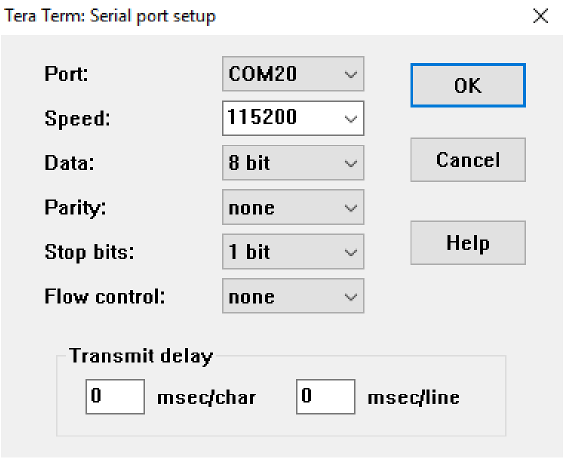
Answerback:

□ Auto switch (VT<->TEK)

Coding (receive): UTF-8

Coding (transmit): UTF-8

locale: american



Tera Term: Serial port setup

Port: COM20

Speed: 115200

Data: 8 bit

Parity: none

Stop bits: 1 bit

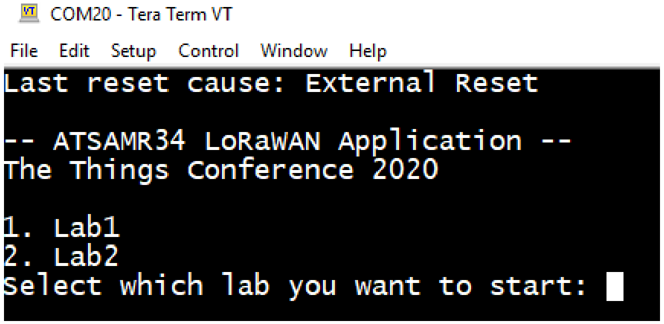
Flow control: none

Transmit delay

0 msec/char 0 msec/line

Run the Application (1/2)

- **Press SAMR34 Xpro Reset button**



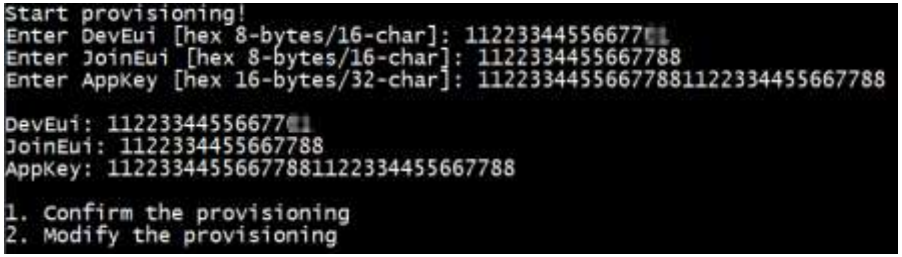
```
Last reset cause: External Reset

-- ATSAMR34 LoRaWAN Application --
The Things Conference 2020

1. Lab1
2. Lab2
Select which lab you want to start:
```

- **From the console, press ‘1’ to Select Lab1**

- **Manually provision your device by entering :**
  - DevEUI (8 Bytes / 16 Char)
  - AppEUI (8 Bytes / 16 Char)
  - AppKey (16 Bytes / 32 Char)

Provided within the appendix sheet

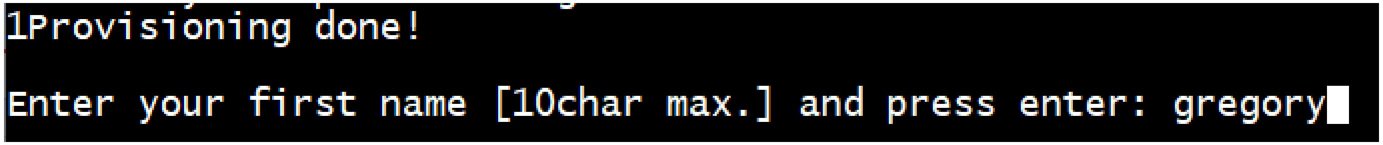
- **Press ‘1’ to confirm your inputs**



```
Start provisioning!
Enter DevEui [hex 8-bytes/16-char]: 11223344556677[redacted]
Enter JoinEui [hex 8-bytes/16-char]: 1122334455667788
Enter AppKey [hex 16-bytes/32-char]: 11223344556677881122334455667788

DevEui: 11223344556677[redacted]
JoinEui: 1122334455667788
AppKey: 11223344556677881122334455667788

1. Confirm the provisioning
2. Modify the provisioning
```

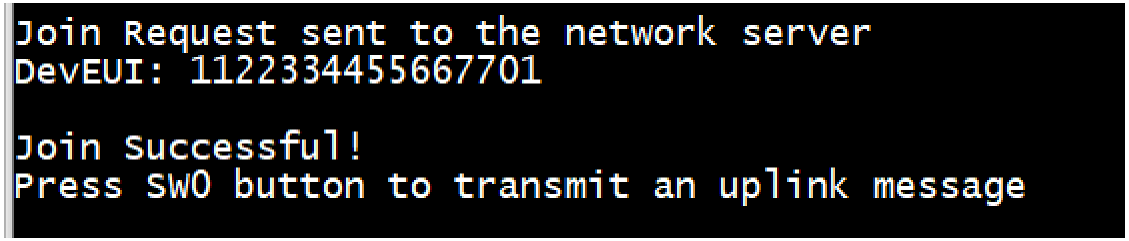
Run the Application (2/2)

- **Enter your first name (10char max.) and press enter:**



```
1Provisioning done!

Enter your first name [10char max.] and press enter: gregory
```

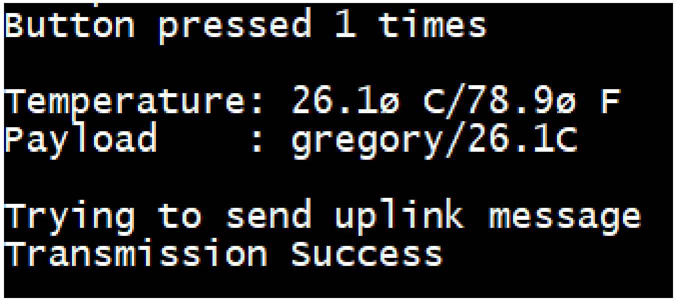
- **Your device should join the network**



```
Join Request sent to the network server
DevEUI: 1122334455667701

Join Successful!
Press SW0 button to transmit an uplink message
```

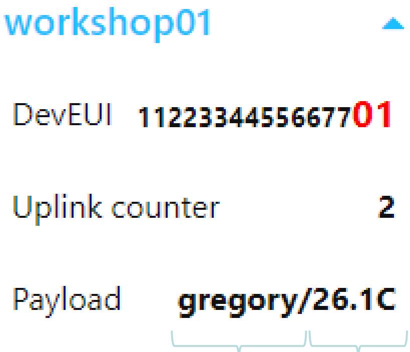
Data Visualization

- **Press SAMR34 Xpro SW0 button to transmit an uplink message**



```
Button pressed 1 times

Temperature: 26.1ø C/78.9ø F
Payload     : gregory/26.1C

Trying to send uplink message
Transmission Success
```

- **Observe the result on the dashboard**



workshop01

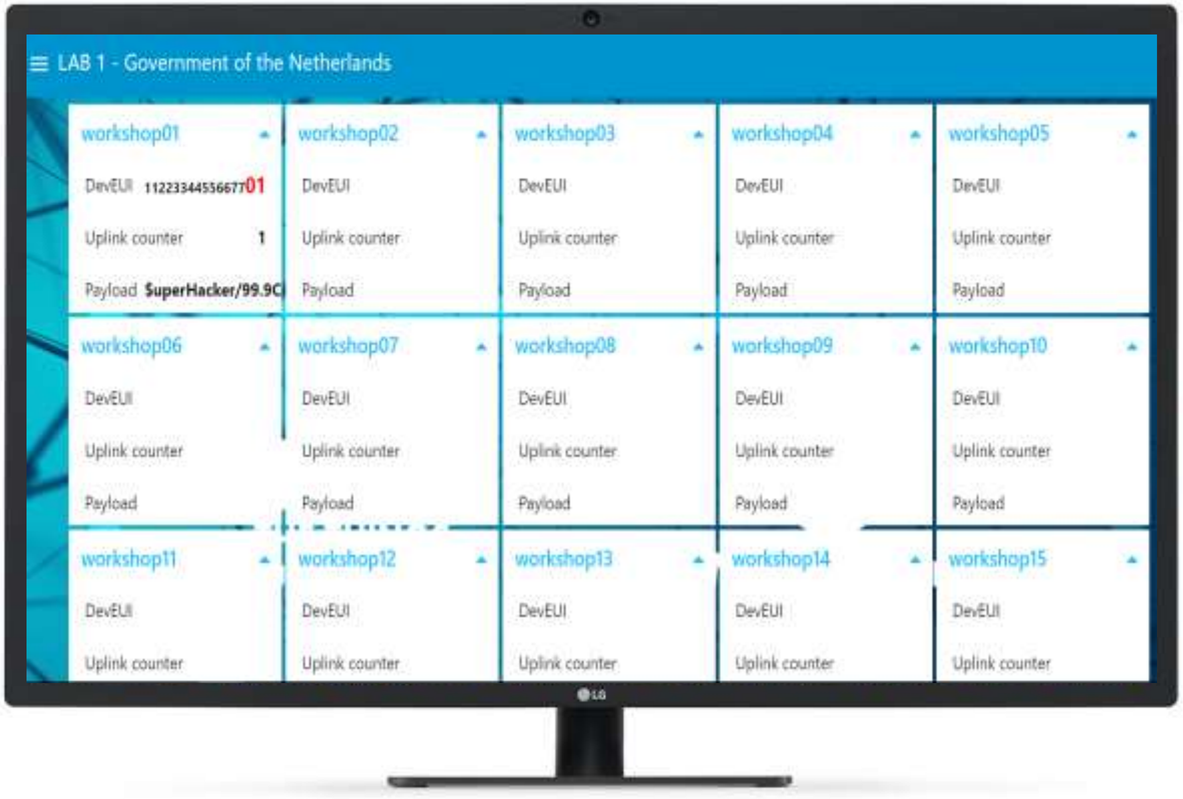
DevEUI 1122334455667701

Uplink counter 2

Payload gregory/26.1C

First_name Device temperature

But…



LAB 1 - Government of the Netherlands

workshop01
DevEUI 112233445566770**1**
Uplink counter 1
Payload $uperHacker/99.9C

workshop02
DevEUI
Uplink counter
Payload

workshop03
DevEUI
Uplink counter
Payload

workshop04
DevEUI
Uplink counter
Payload

workshop05
DevEUI
Uplink counter
Payload

workshop06
DevEUI
Uplink counter
Payload

workshop07
DevEUI
Uplink counter
Payload

workshop08
DevEUI
Uplink counter
Payload

workshop09
DevEUI
Uplink counter
Payload

workshop10
DevEUI
Uplink counter
Payload

workshop11
DevEUI
Uplink counter

workshop12
DevEUI
Uplink counter

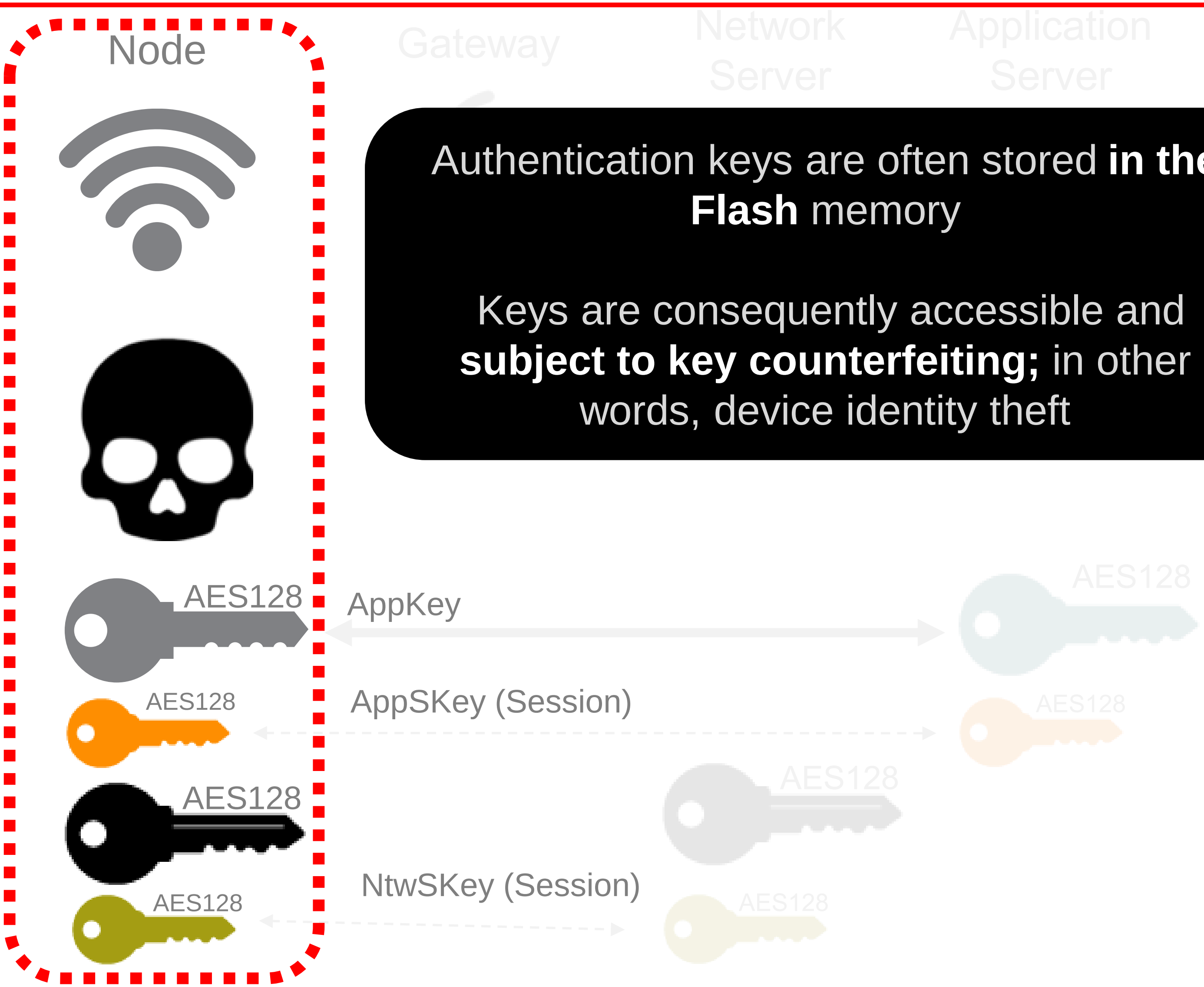
workshop13
DevEUI
Uplink counter

workshop14
DevEUI
Uplink counter

workshop15
DevEUI
Uplink counter

Nicolas, aka « $uperHacker » sniffed the keys of one of our sensor, and now spoofs wrong data on our dashboard using a clone sensor

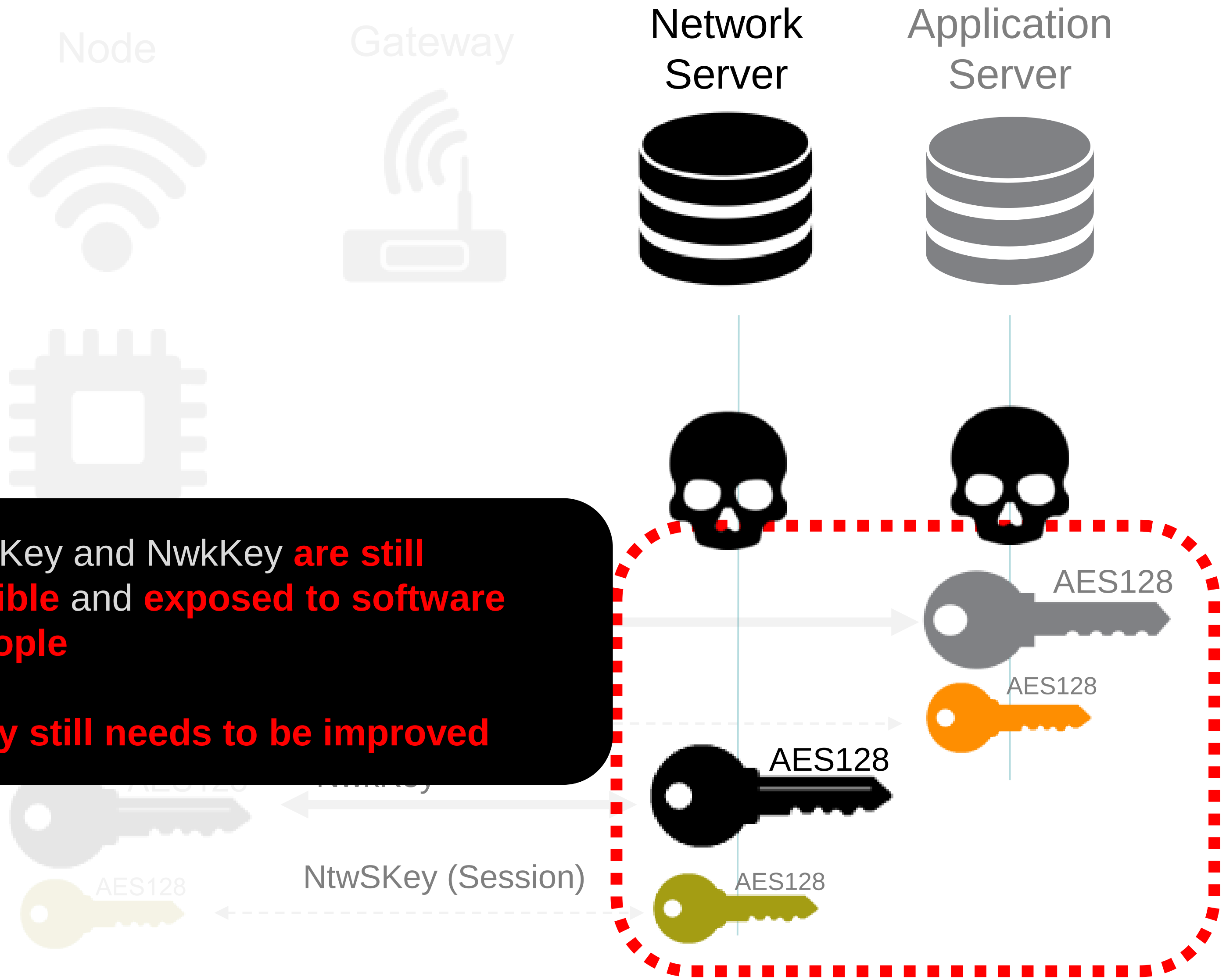
LoRaWAN Device Vulnerability



Authentication keys are often stored **in the Flash** memory

Keys are consequently accessible and **subject to key counterfeiting;** in other words, device identity theft

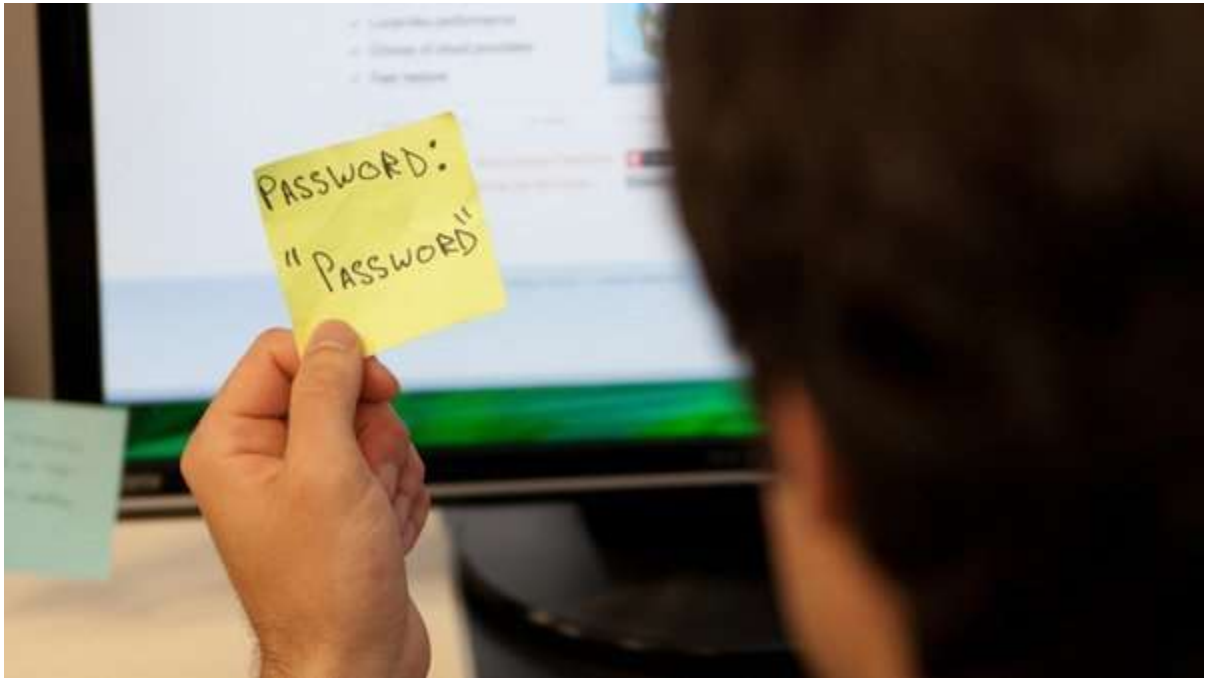
Backend Vulnerability

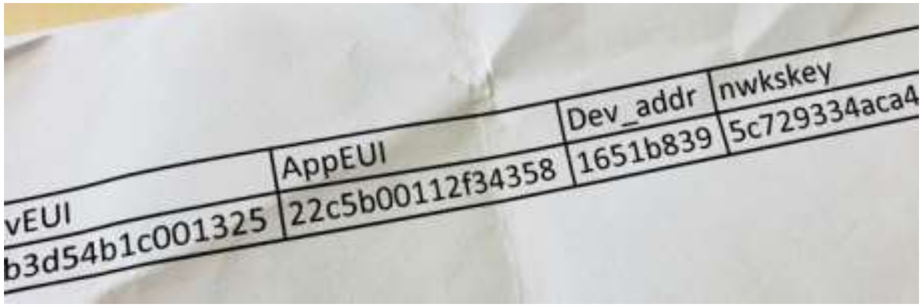


Yet AppKey and NwkKey **are still accessible** and **exposed to software and people**

Security still needs to be improved

User Vulnerability





vEUI	AppEUI	Dev_addr	nwkskey
b3d54b1c001325	22c5b00112f34358	1651b839	5c729334aca4

Best Security Practices for Keys Handling

- **The Goal to Reach : Build a chain of TRUST**
  - Create a unique, trusted and managed identity

1 **Isolate private keys from users**

Humans are the most unpredictable security risk

2 **Isolate private keys from software and firmware**

Any unprotected MCU or MPU is hackable and any secrets stored in code are vulnerable

3 **Isolate key manipulation from the manufacturing phase**

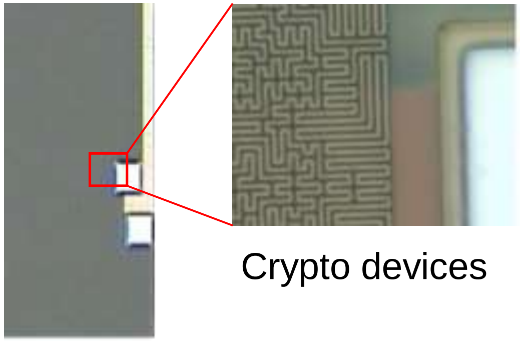
Not only from the supply chain equipment but also from the users in the supply chain

4 **Keep critical crypto-primitives where the keys are: isolated**

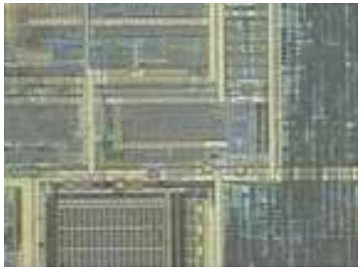
If algorithms dealing with keys are in a separate container, backdoors appear

How Keys Are Protected Matters

- **Strong multi-level HW security**
  - Active shield over entire chip
  - All memories internally encrypted
  - Data independent crypto execution
  - Randomized math operations
  - Internal state consistency checking
  - Voltage tampers, isolated power rail
  - Internal clock generation
  - Secure test methods, no JTAG
  - No debug probe points or test pads



Crypto devices

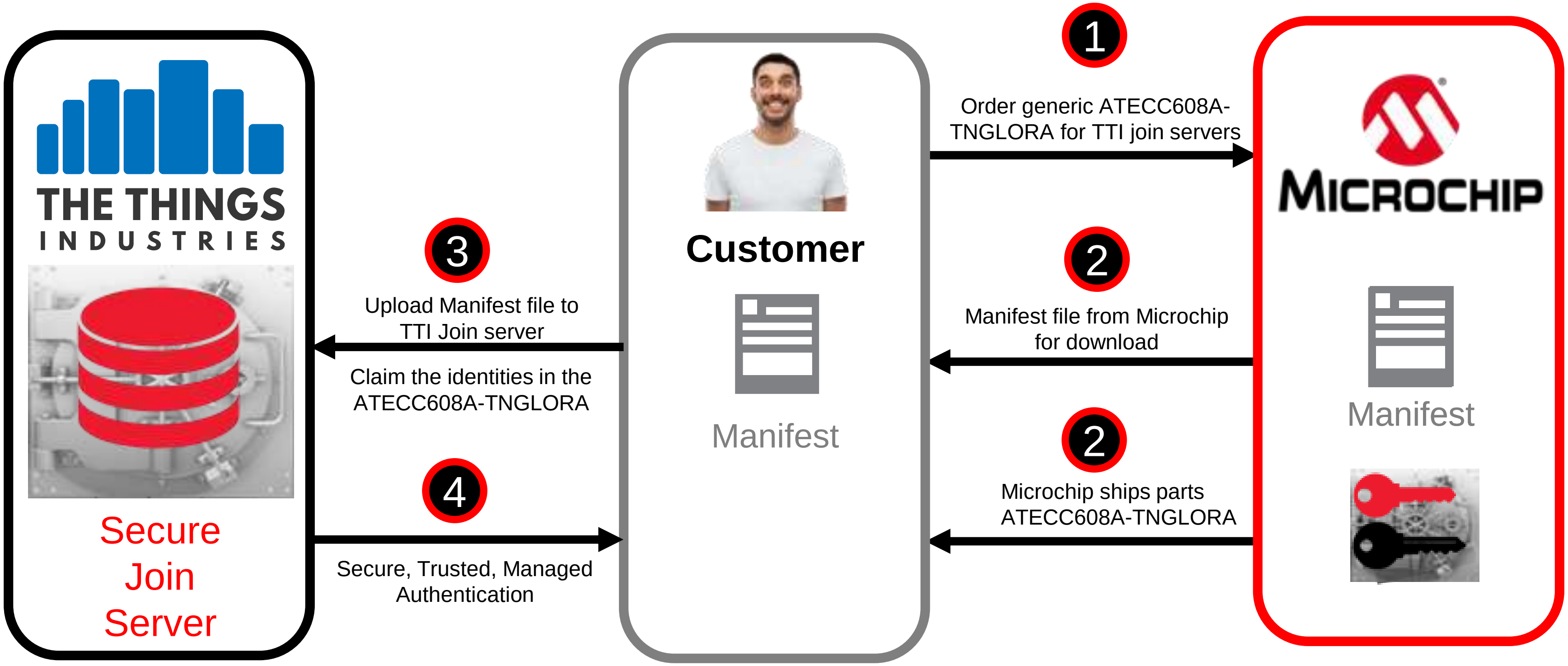


Standard devices

- **Designed to defend against**
  - Microprobe attacks
  - Timing attacks
  - Emissions analysis attacks
  - Fault, invalid command attacks
  - Power cycling, clock glitches

- **ECC608 Overview**
  - Provides secure storage and execution environment for keys
    - Symmetric (SHA256) and Asymmetric (elliptic curve)
  - Supports NIST P-256 curve
    - a.k.a. secp256r1, prime256v1
  - 10.5Kb storage across 16 slots
  - High-quality internal RNG
  - Supports SHA256, ECDSA, ECDH, various KDF, and AES algorithms

A Simple Onboarding



THE THINGS INDUSTRIES
Secure Join Server
3
Upload Manifest file to TTI Join server
Claim the identities in the ATECC608A-TNGLORA
4
Secure, Trusted, Managed Authentication
Customer
Manifest
1
Order generic ATECC608A-TNGLORA for TTI join servers
2
Manifest file from Microchip for download
2
Microchip ships parts ATECC608A-TNGLORA
MICROCHIP
Manifest

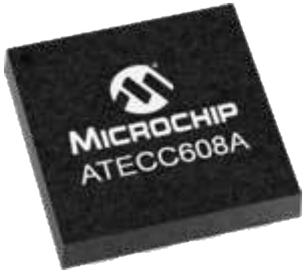
Secure Authentication for LoRaWAN

Pre-provisioned
Secure Key Storage

Secure Provisioning
Service from Microchip

Bundled with one year of
TTI Join Server service

TTI Join Server
Re-keying



ATECC608A-TNGLORA

THE THINGS INDUSTRIES

Join
Server

www.microchip.com/ATECC608A-TNGLORA

Feedbacks from Management

Complexity is completely removed during development and manufacturing

Re-keying is possible give me flexibility to choose another network server

On boarding is easier, safer, simpler. And cost-effective

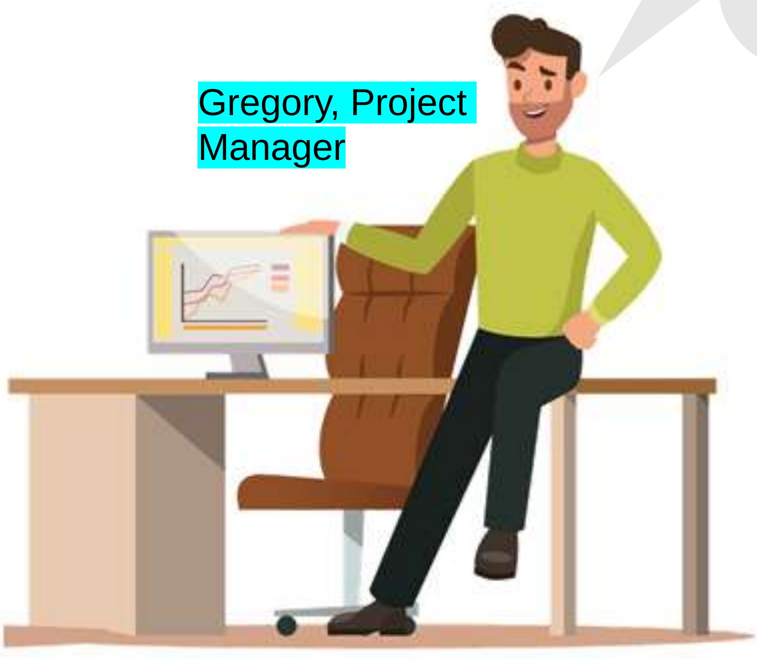
Security is not a problem but THE solution thanks to a secure Element and TTI end to end approach.

But first and foremost, my application is secured !!!
Our brand and reputation will not be at risk

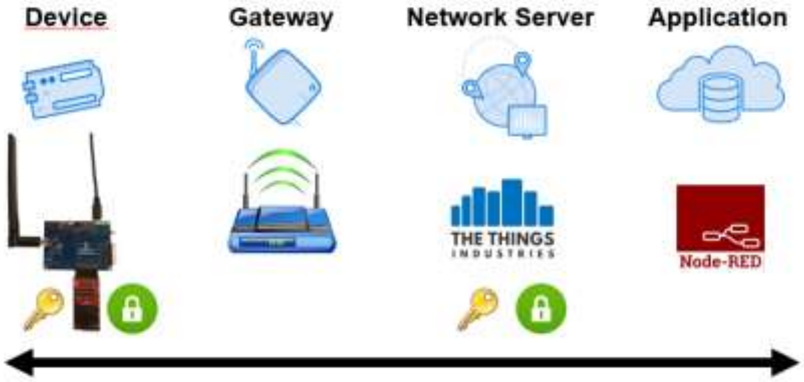
Clayton, now a happy Boss

Lab 2

Ok guys, let’s follow the new guidelines from Clayton, adding ATECC608 Secure Element :
1) Set-up your TTI session on their web portal (Console). And claim the device using a manifest
2) Device gets connected to TTI Network Server
3) Validate that every sensors in the field reports its temperature properly back to our Company dashboard.



Gregory, Project Manager

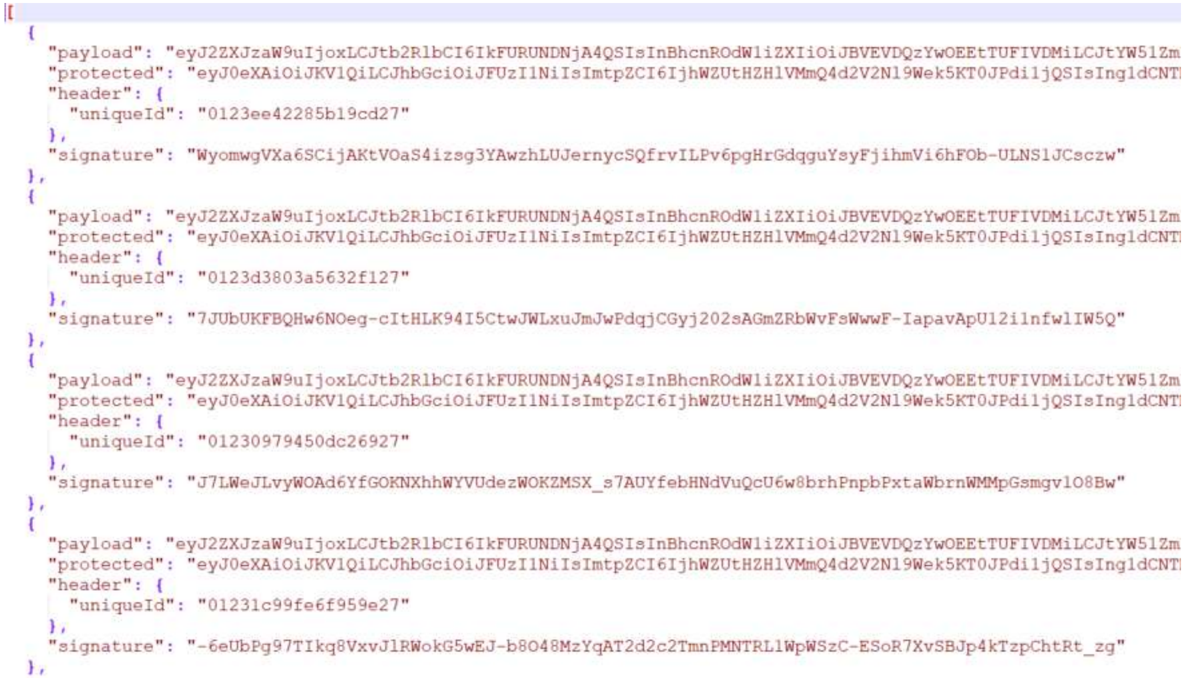


Lab Material

- The Things Industries Network Server Account
- The Things Industries Join Server Account
- A manifest file
- A SAMR34 Xpro board pre-loaded with an ASF application specifically written for this workshop
- A micro-USB cable
- An RF antenna
- A pre-provisioned ECC608A-TNGLORA inserted in a socket board

Secure Element
The Manifest File

- **Design to convey the unique information about a group of secure elements including unique ID, public keys and certificates**
- **The base format is an array of JSON objects**

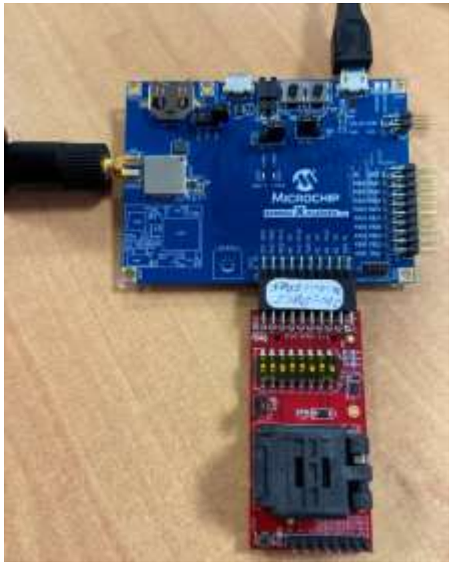


```
[
  {
    "payload": "eyJ2ZXJzaW9uIjoxLCJtb2RlbCI6IkFURUNDNjA4QSIsInBhcnROdW1iZXIiOiJBVEVDQzYwOEEtTUFIVDMiLCJtYW51Zm
    "protected": "eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsImtpZCI6IjhWZUtHZHlVMmQ4d2V2N19Wek5KT0JPdiljQSIsIngldCNT
    "header": {
      "uniqueId": "0123ee42285b19cd27"
    },
    "signature": "WyomwgVXa6SCijAKtVOaS4izsg3YAwzhLUJernycSQfrvILPv6pgHrGdqguYsyFjihmVi6hFOb-ULNSlJCsczw"
  },
  {
    "payload": "eyJ2ZXJzaW9uIjoxLCJtb2RlbCI6IkFURUNDNjA4QSIsInBhcnROdW1iZXIiOiJBVEVDQzYwOEEtTUFIVDMiLCJtYW51Zm
    "protected": "eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsImtpZCI6IjhWZUtHZHlVMmQ4d2V2N19Wek5KT0JPdiljQSIsIngldCNT
    "header": {
      "uniqueId": "0123d3803a5632f127"
    },
    "signature": "7JUbUKFBQHw6NOeg-cItHLK94I5CtwJWLxuJmJwPdqjCGyj202sAGmZRbWvFsWwwF-IapavApU12ilnfwlIW5Q"
  },
  {
    "payload": "eyJ2ZXJzaW9uIjoxLCJtb2RlbCI6IkFURUNDNjA4QSIsInBhcnROdW1iZXIiOiJBVEVDQzYwOEEtTUFIVDMiLCJtYW51Zm
    "protected": "eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsImtpZCI6IjhWZUtHZHlVMmQ4d2V2N19Wek5KT0JPdiljQSIsIngldCNT
    "header": {
      "uniqueId": "01230979450dc26927"
    },
    "signature": "J7LWeJLvyWOAd6YfGOKNXhhWYVUdezWOKZMSX_s7AUYfebHNdVuQcU6w8brhPnpbPxtaWbrnWMMpGsmgv108Bw"
  },
  {
    "payload": "eyJ2ZXJzaW9uIjoxLCJtb2RlbCI6IkFURUNDNjA4QSIsInBhcnROdW1iZXIiOiJBVEVDQzYwOEEtTUFIVDMiLCJtYW51Zm
    "protected": "eyJ0eXAiOiJKV1QiLCJhbGciOiJFUzI1NiIsImtpZCI6IjhWZUtHZHlVMmQ4d2V2N19Wek5KT0JPdiljQSIsIngldCNT
    "header": {
      "uniqueId": "01231c99fe6f959e27"
    },
    "signature": "-6eUbPg97TIkq8VxvJlRWokG5wEJ-b8O48MzYqAT2d2c2TmnPMNTRL1WpWSzC-ESoR7XvSBJp4kTzpChtRt_zg"
  },
```

https://github.com/MicrochipTech/secure_lorawan_with_tti

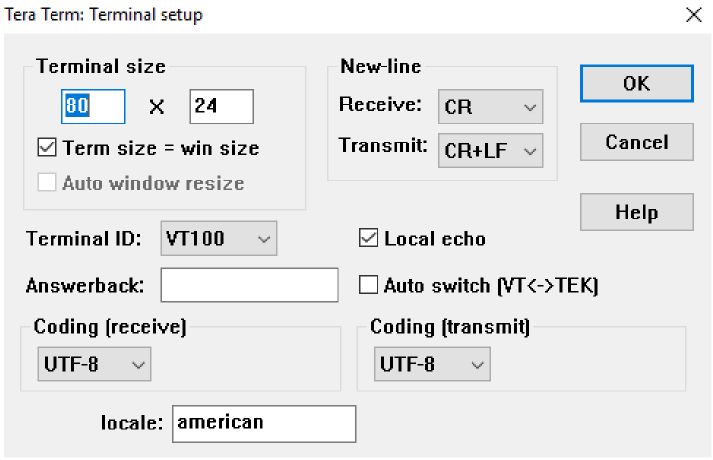
Hardware Setup

- Connect ECC608A Socket board to SAMR34 Xpro EXT3
- Plug the antenna and always make sure you have the antenna plugged to your SAMR34 Xpro board before powering it up
- Connect your SAMR34 Xpro board to the computer through the micro-USB cable. USB cable must be connected to the EDBG USB connector of the kit.
- Wait for USB driver installation and COM port mounting. The USB port powers the board and enables the user to communicate with the kit.



Serial Console Setup

- Open Serial Console (e.g. TeraTerm)
- Configure Terminal setup
- Configure Serial port setup: COMxx 115200 bps / 8 / N / 1



Tera Term: Terminal setup

Terminal size

80 × 24

☑ Term size = win size

☐ Auto window resize

New-line

Receive: CR

Transmit: CR+LF

Terminal ID: VT100

☑ Local echo

Answerback:

☐ Auto switch (VT<->TEK)

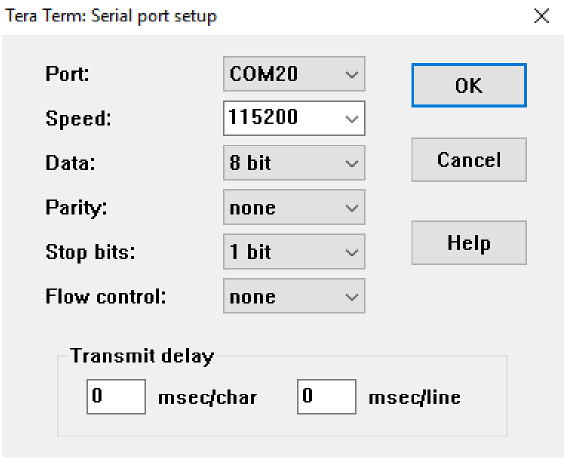
Coding (receive)

UTF-8

Coding (transmit)

UTF-8

locale: american



Tera Term: Serial port setup

Port: COM20

Speed: 115200

Data: 8 bit

Parity: none

Stop bits: 1 bit

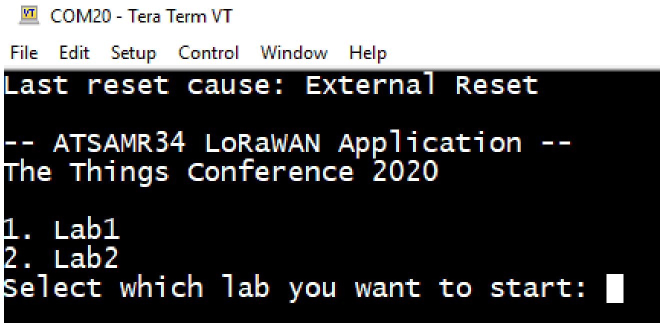
Flow control: none

Transmit delay

0 msec/char 0 msec/line

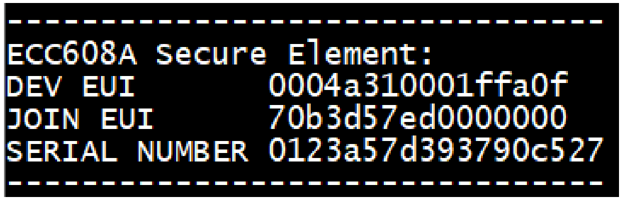
Record your device IDs

- **Press SAMR34 Xpro Reset button**



```
Last reset cause: External Reset

-- ATSAMR34 LoRaWAN Application --
The Things Conference 2020

1. Lab1
2. Lab2
Select which lab you want to start:
```

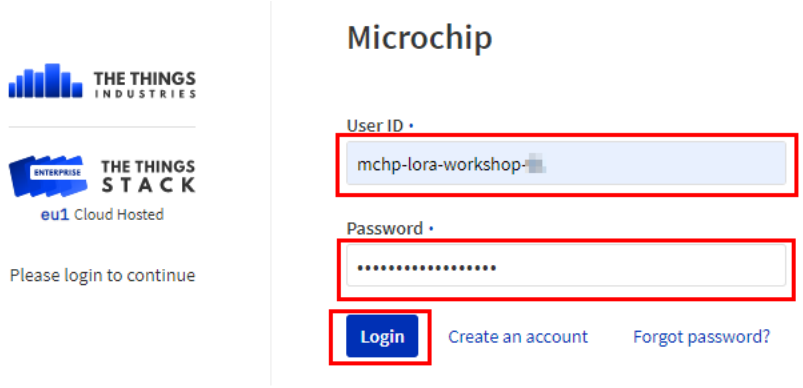
- **From the console, press ‘2’ to Select Lab 2**
- **Observe the following identifiers coming from the ATECC608A Secure Element**
- **Record your own DevEUI and Serial number**
- **Ask for the manifest file which match your set of identifiers**



```
--------------------------------
ECC608A Secure Element:
DEV EUI       0004a310001ffa0f
JOIN EUI      70b3d57ed0000000
SERIAL NUMBER 0123a57d393790c527
--------------------------------
```

TTI Join Server Login

- **Open the TTI Join Server Console: https://microchip.join.cloud.thethings.industries/**
- **Login by using the TTI Credentials provided within the appendix sheet**



Please login to continue

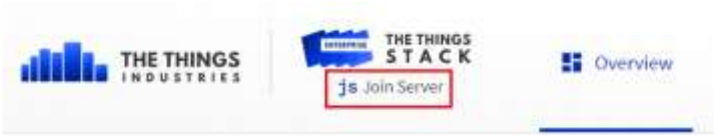
Microchip

User ID •

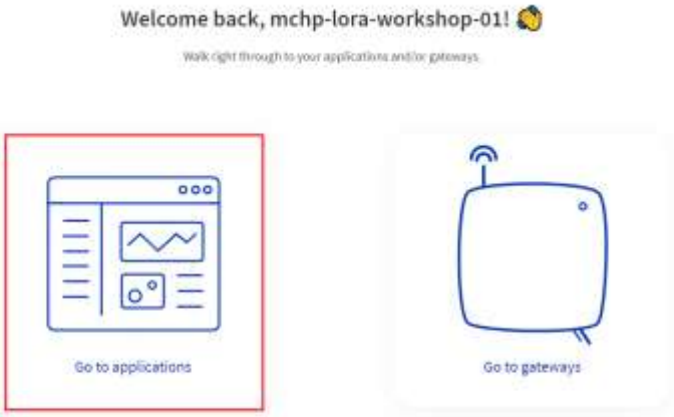
mchp-lora-workshop-[redacted]

Password •

••••••••••••••••••



- **Select Go to applications**

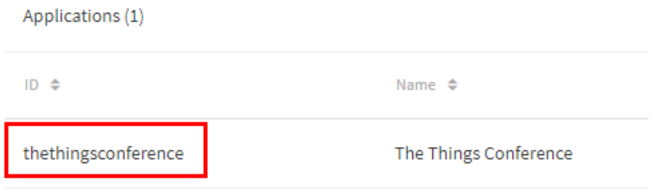


Welcome back, mchp-lora-workshop-01! 👋

Walk right through to your applications and/or gateways.

Select Application

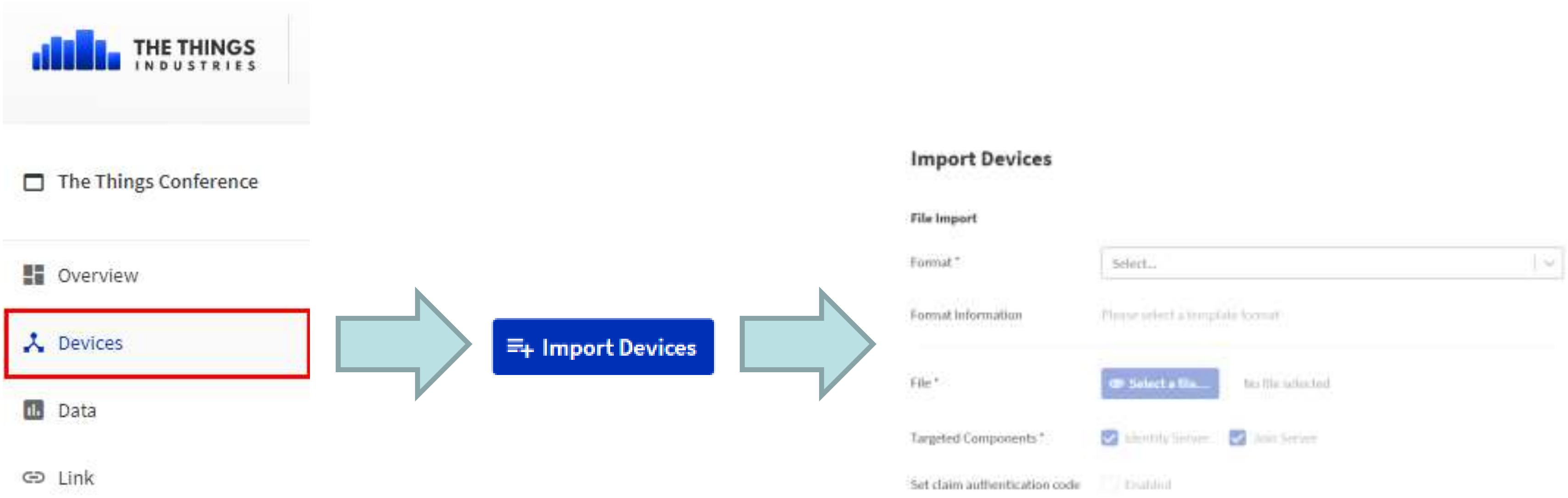
- **Select ‘thethingsconference’ application**



Applications (1)

ID	Name
thethingsconference	The Things Conference

- **Go to “Devices” in the left menu and click on “+ Import Device”**



Import Devices

File Import

Format * Select...

Format Information Please select a template format

File * Select a file... No file selected

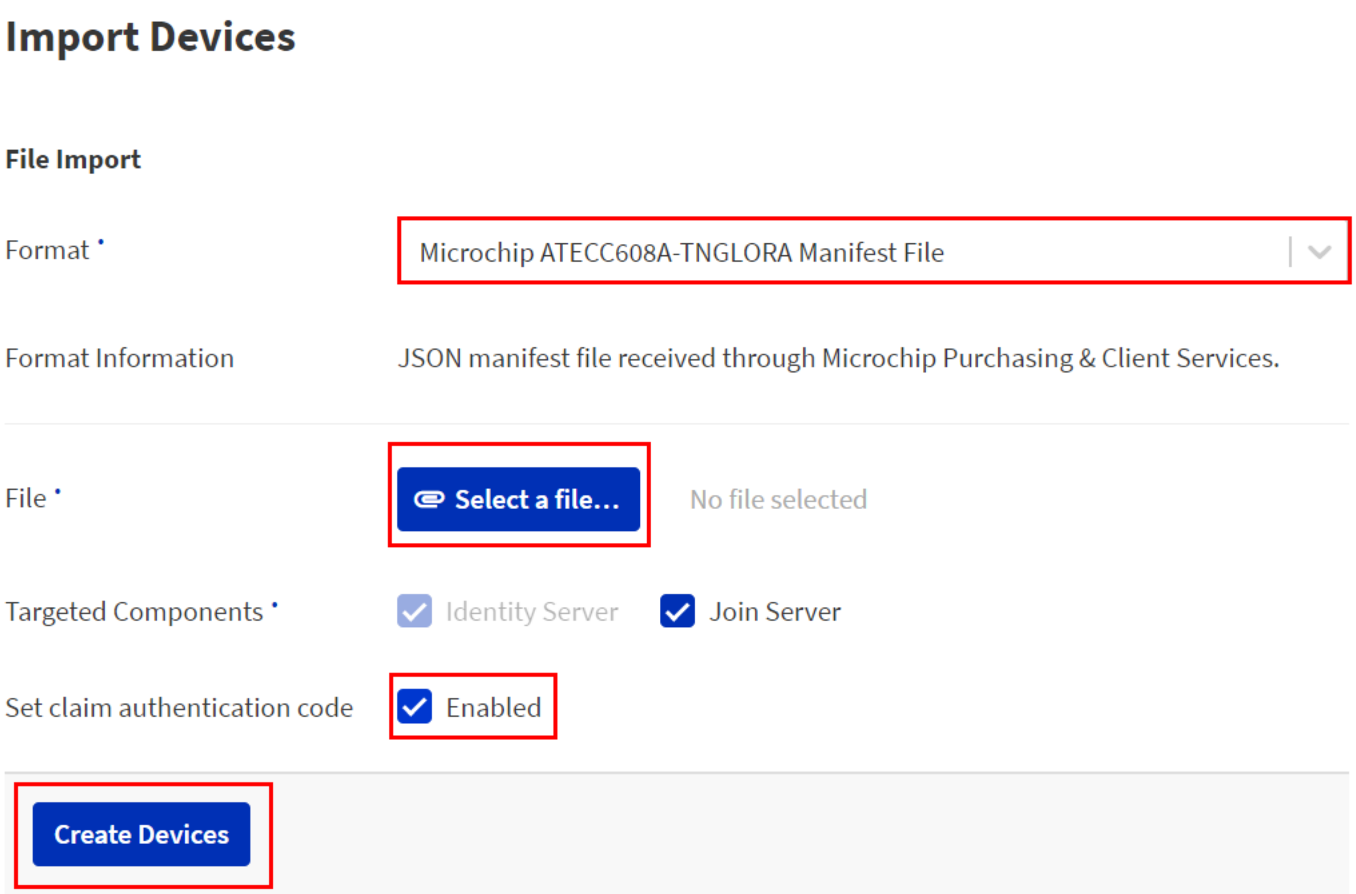
Targeted Components * ☑ Identity Server ☑ Join Server

Set claim authentication code □ Enabled

Device Claiming

Import Device in the Join Server

- https://enterprise.thethingsstack.io/v3.3.2/guides/claim-atecc608a/



Import Devices

File Import

Format • Microchip ATECC608A-TNGLORA Manifest File

Format Information JSON manifest file received through Microchip Purchasing & Client Services.

File • Select a file... No file selected

Targeted Components • ☑ Identity Server ☑ Join Server

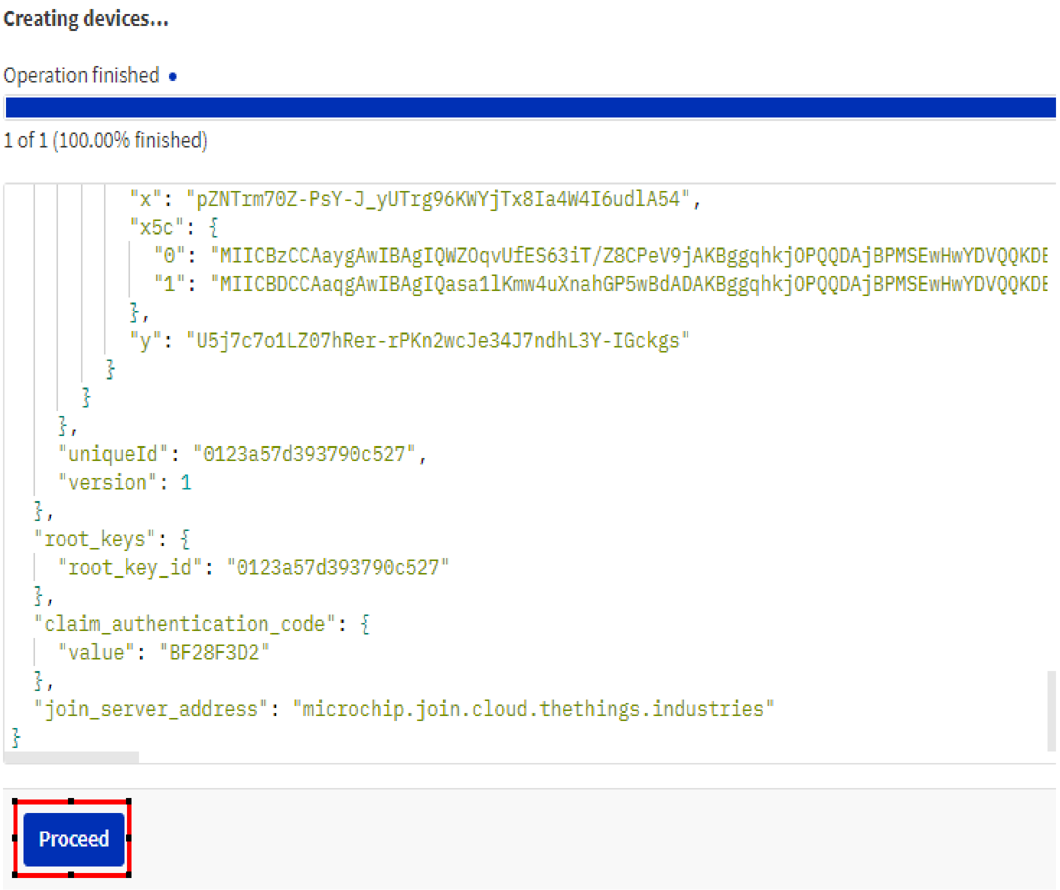
Set claim authentication code ☑ Enabled

Create Devices

Device Claiming

Import Device in the Join Server

- **Your secure element is now claimed in your application.
The secure element cannot be claimed by anyone else until you delete the device.**



Creating devices...

Operation finished

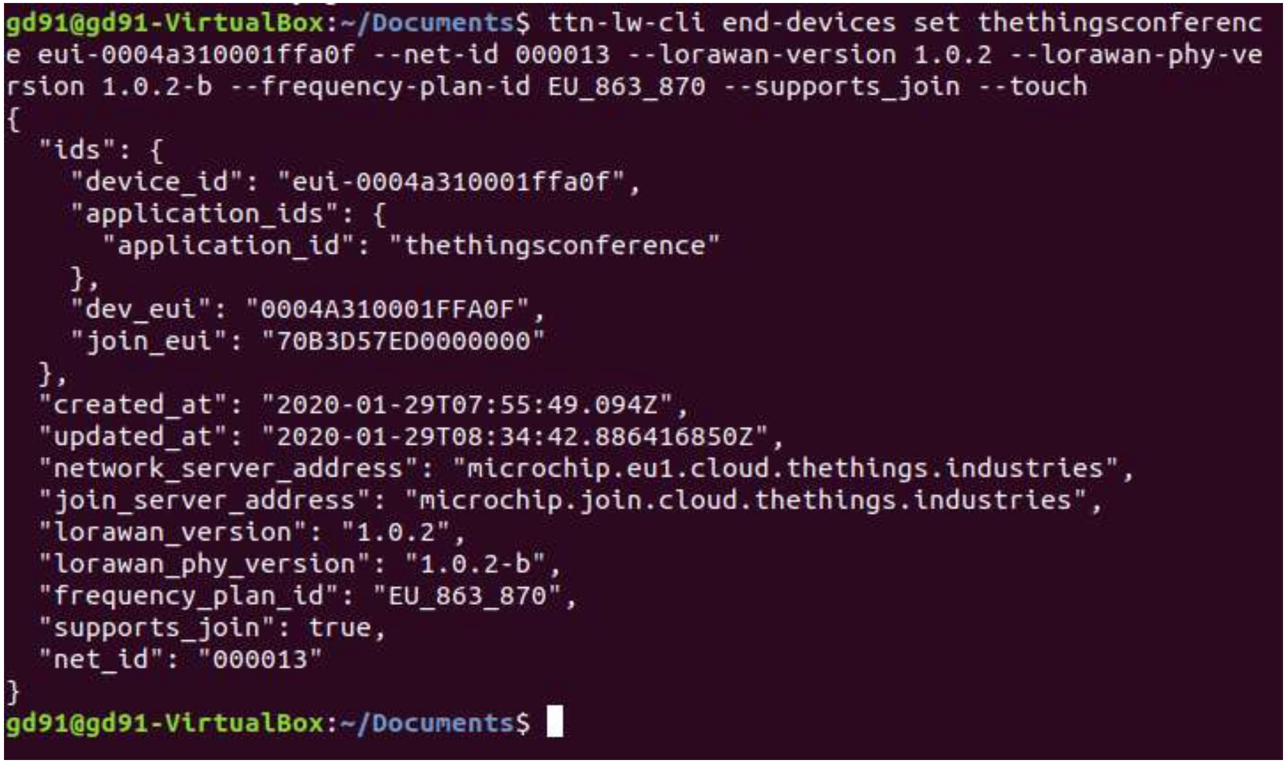
1 of 1 (100.00% finished)

```
          "x": "pZNTrm70Z-PsY-J_yUTrg96KWYjTx8Ia4W4I6udlA54",
          "x5c": {
            "0": "MIICBzCCAaygAwIBAgIQWZOqvUfES63iT/Z8CPeV9jAKBggqhkjOPQQDAjBPMSEwHwYDVQQKDE
            "1": "MIICBDCCAaqgAwIBAgIQasa1lKmw4uXnahGP5wBdADAKBggqhkjOPQQDAjBPMSEwHwYDVQQKDE
          },
          "y": "U5j7c7o1LZ07hRer-rPKn2wcJe34J7ndhL3Y-IGckgs"
        }
      }
    },
    "uniqueId": "0123a57d393790c527",
    "version": 1
  },
  "root_keys": {
    "root_key_id": "0123a57d393790c527"
  },
  "claim_authentication_code": {
    "value": "BF28F3D2"
  },
  "join_server_address": "microchip.join.cloud.thethings.industries"
}
```

Device Registration

Register device in the Network Server

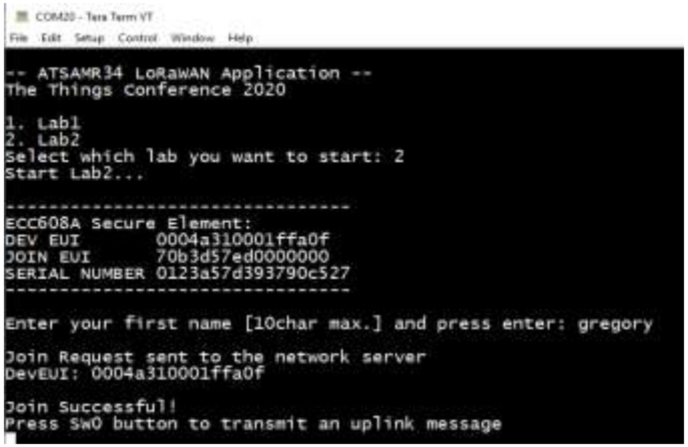
- Claiming the secure element only create device on the Join Server
- CLI is required to activate the device in the Network Server
- https://enterprise.thethingsstack.io/v3.3.2/guides/cloud-hosted/tti-join-server/activate-devices-cloud-hosted/



```
gd91@gd91-VirtualBox:~/Documents$ ttn-lw-cli end-devices set thethingsconferenc
e eui-0004a310001ffa0f --net-id 000013 --lorawan-version 1.0.2 --lorawan-phy-ve
rsion 1.0.2-b --frequency-plan-id EU_863_870 --supports_join --touch
{
  "ids": {
    "device_id": "eui-0004a310001ffa0f",
    "application_ids": {
      "application_id": "thethingsconference"
    },
    "dev_eui": "0004A310001FFA0F",
    "join_eui": "70B3D57ED0000000"
  },
  "created_at": "2020-01-29T07:55:49.094Z",
  "updated_at": "2020-01-29T08:34:42.886416850Z",
  "network_server_address": "microchip.eu1.cloud.thethings.industries",
  "join_server_address": "microchip.join.cloud.thethings.industries",
  "lorawan_version": "1.0.2",
  "lorawan_phy_version": "1.0.2-b",
  "frequency_plan_id": "EU_863_870",
  "supports_join": true,
  "net_id": "000013"
}
gd91@gd91-VirtualBox:~/Documents$ 
```

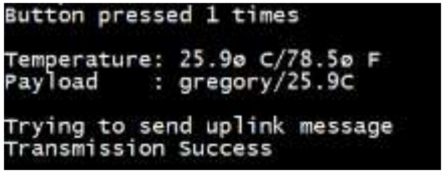
Join and Transmit

- From the console, enter your first name and press enter
- Your device should successfully join the network



```
-- ATSAMR34 LoRaWAN Application --
The Things Conference 2020

1. Lab1
2. Lab2
Select which lab you want to start: 2
Start Lab2...

--------------------------------
ECC608A Secure Element:
DEV EUI       0004a310001ffa0f
JOIN EUI      70b3d57ed0000000
SERIAL NUMBER 0123a57d393790c527
--------------------------------

Enter your first name [10char max.] and press enter: gregory

Join Request sent to the network server
DevEUI: 0004a310001ffa0f

Join Successful!
Press SW0 button to transmit an uplink message
```

- Press SAMR34 Xpro SW0 button to transmit an uplink message



```
Button pressed 1 times

Temperature: 25.9ø C/78.5ø F
Payload     : gregory/25.9C

Trying to send uplink message
Transmission Success
```

- Observe the result on the dashboard and confirm you can visualize your data

Conclusion

We have long term solution, fully supported by Microchip and TTI. Their solutions (SAMR34 + ATECC608) are in production and available now

It is secure and robust. But also cost effective. On boarding is easy and fast. Great solution for development and manufacturing

Congratulation, team. Management has validated our project & launched production

Solution works perfectly. It is fully CE/FCC/IC certified

Jeroen

Me

Team has made it !
We now have a
working solution,
ready for production

Gregory, Project
Manager

Johan

Take Away

- Good security is not expensive, bad security is! Key Storage and Key Management are the cornerstones for a Secure for IoT Solution

- Pre-Provisioned Secure Element on a LoRaWAN node makes your application secure and simplify on boarding along manufacturing with a cost-effective approach

- Secure element can add additional functionality such as Secure Boot, FUOTA verification, re-keying

- Microchip has end to end LoRaWan approach with SAMR34 LoRa MCU and ATECC608 Secure Element, enabling Smart Connected and Secure IoT

Thank you for your time!

MICROCHIP

THE THINGS INDUSTRIES

Meet us at embedded world Nuremberg, Germany
February 27, 2020

https://github.com/MicrochipTech/secure_lorawan_with_tti