Quick Start Guide

Security Starter Kit with i.MX 8X and OPTIGA™ TPM 2.0

Date: November 5, 2020 | Version 1.0
FINAL

CONTENTS

1 INTRODUCTION 3
1.1 Purpose of the Document 3
1.2 Prerequisite 3
1.3 Scope of Detailed Design 3
2 INSTALLATION STEPS 4
2.1 Hardware setup – Security Starter Kit with i.MX 8X and OPTIGA™ TPM 2.0 4
2.2 Software setup – Security Starter Kit with i.MX 8X and OPTIGA™ TPM 2.0 5
2.2.1 AWS Account creation and Arrow Cloud Connect tool configuration 5
2.2.2 Software Setup on Linux Host PC (For Linux Users) 5
2.2.3 Software Setup on Windows Host PC (For Windows Users) 6
2.2.4 Wi-Fi Setup on the AI_ML Board 7
2.2.5 File Sharing Setup between Host PC and AI_ML Board 8
2.3 CA Registration on SSK Cloud Connect 9
2.4 Demo Setup 12
2.4.1 AWS Traffic Light Demo configuration and setup 12
2.4.2 Deploying Greengrass Group 16
2.4.3 Run AWS Traffic Light Demo 18
2.4.4 Demo Result 19
2.4.5 Demo Inference 21

DEFINITION, ACRONYMS AND ABBREVIATIONS

Definition/Acronym/Abbreviation	Description
AI_ML board	Arrow 96boards I.MX8X_AI_ML (Artificial intelligence and Machine Learning) board featuring the NXP i.MX 8X MPU
AWS	Amazon Web Services
CA	Certificate Authority
GG	AWS IoT Greengrass
SSK	Security Starter Kit
TPM	Trusted Platform Module
SBC	Single-board computer

1 INTRODUCTION

1.1 Purpose of the Document

The Quick Start guide for the Security Starter Kit with i.MX 8X and OPTIGA™ TPM2.0 will provide an example and showcase the functionality of AWS IoT Greengrass on the Arrow 96boards I.IMX8X_AI_ML Board using OPTIGA™ TPM 2.0 (Infineon SLB9670 or SLM9670). This demo also exhibits provisioning, authentication and secure communication features between the gateway/edge compute solution and the Cloud.

1.2 Prerequisite

Below are the list of Hardware and Software needed to enable the demonstration of the AWS IoT Greengrass and OPTIGA™ TPM 2.0 security,

- Security Starter Kit Setup will require following
  - Arrow 96boards I.IMX8X_AI_ML SBC
  - Arrow 96boards Tresor Mezzanine card (with the OPTIGA™ TPM2.0 installed)
  - SD card – 16GB
  - MicroUSB debug cable
  - Power Supply;
    - MEAN WELL GST60A12-P1J
    - 5.5/2.1mm to 4.75/1.7mm cable DC plug converter
- Linux PC with Minicom OR Windows PC with Putty and winscp
- Internet connectivity (Wi-Fi/Ethernet) of Board and Host PC should be on same Network.

1.3 Scope of Detailed Design

Integration of AWS IoT Greengrass with OPTIGA™ TPM 2.0 to provide hardware-based endpoint device security. This integration ensures the use of private key to establish device identity, which is securely stored in tamper-proof hardware devices, which prevents the device from being compromised, impersonated and other malicious activities.

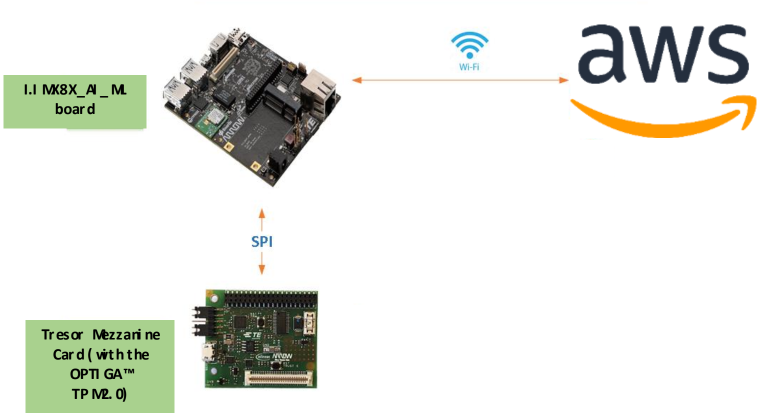


Figure 1: Setup Schematic

2 INSTALLATION STEPS

2.1 Hardware setup – Security Starter Kit with i.MX 8X and OPTIGA™ TPM 2.0

The i.MX 8X-SSK is shipped from the factory, pre-configured with the SD Card installed. In case the user would like to refer the hardware setup, one can do so in the i.MX_8X-SSK Developers Guide.pdf Section 3.1 for the Hardware Setup details.
https://www.arrow.com/en/products/imx-8x-ssk/arrow-development-tools

1. Connect the power supply and MicroUSB cable to Host PC as shown below:

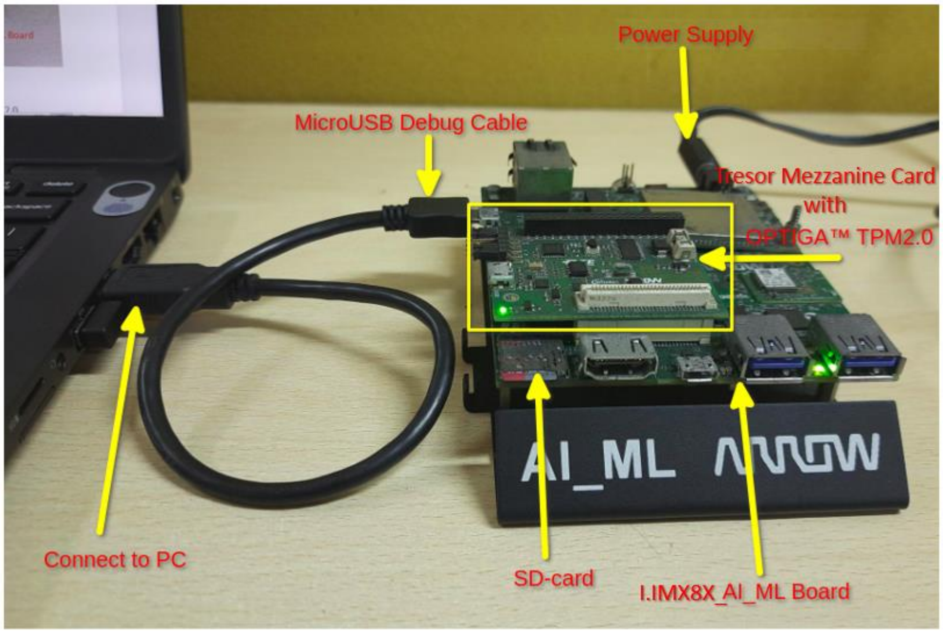


Figure 2: Hardware Setup

2.2 Software setup – Security Starter Kit with i.MX 8X and OPTIGA™ TPM 2.0

2.2.1 AWS Account creation and Arrow Cloud Connect tool configuration

The points mentioned below are specific to enabling AWS Cloud Services with the Security Starter Kit and needs to be executed only once. The output from these configuration steps can be reused to connect other Security Starter Kits to AWS Cloud Services. These steps must be completed prior to running the included demo.

1. It is presumed that the user has an AWS Management Console account needed to complete the steps listed below. Otherwise, one has to create an account; https://aws.amazon.com/console/

2. Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

   The user must configure a unique EC2 instance, which will provide a unique URL and login credentials tied to your AWS account for the Arrow Cloud Connect Tool.

   The EC2 configuration instructions are outlined in the SSK_Cloud_Connect Quick Start Guide.pdf
   Product Launch page:
   https://www.arrow.com/en/products/imx-8x-ssk/arrow-development-tools

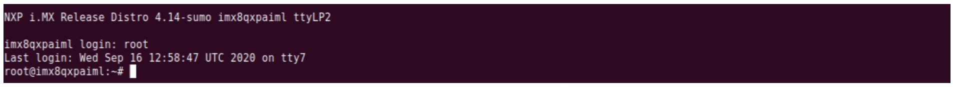
2.2.2 Software Setup on Linux Host PC (For Linux Users)

1. Install console application **minicom on** Linux PC
2. On Linux PC, open Minicom in the Linux PC (For debugging purpose)

```
Linux_PC:~$ sudo minicom -s
```

3. Set baud rate and other setting as per below
   a. Baud rate 115200
   b. Parity none
   c. hardware flow control /software flow control none
   d. Serial device /dev/ttyUSB0
   e. **save setup as dfl**

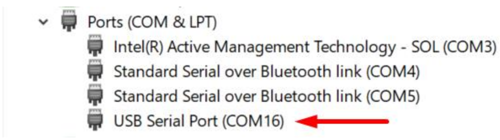
4. After the AI_ML board boots up, it will display the login console on minicom terminal on Linux PC as shown below
5. Username for board is “root” without any password (if asked for).



```
NXP i.MX Release Distro 4.14-sumo imx8qxpaiml ttyLP2

imx8qxpaiml login: root
Last login: Wed Sep 16 12:58:47 UTC 2020 on tty7
root@imx8qxpaiml:~# 
```

2.2.3 Software Setup on Windows Host PC (For Windows Users)

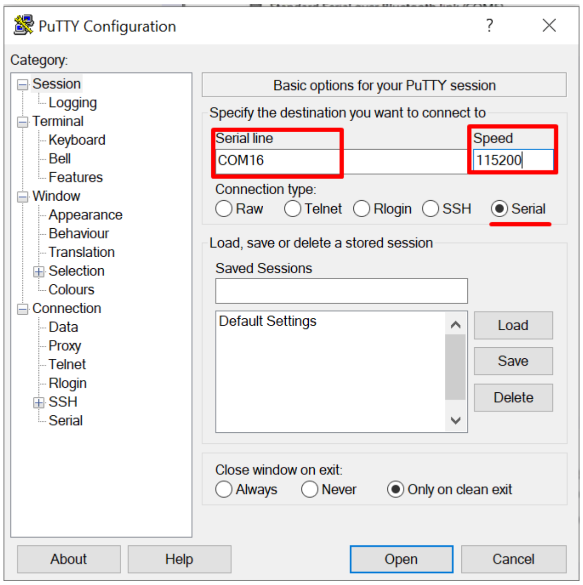
1. Install console application Putty on Windows Host PC
2. Open the Host PC Device Manager Tool and make note of the COM port assigned for the USB connection as shown below



- Ports (COM & LPT)
  - Intel(R) Active Management Technology - SOL (COM3)
  - Standard Serial over Bluetooth link (COM4)
  - Standard Serial over Bluetooth link (COM5)
  - USB Serial Port (COM16)

3. Open Putty application and set the parameters as shown below

Note: Set the COM port using the one assigned by the Device Manager in step #2.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM16

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

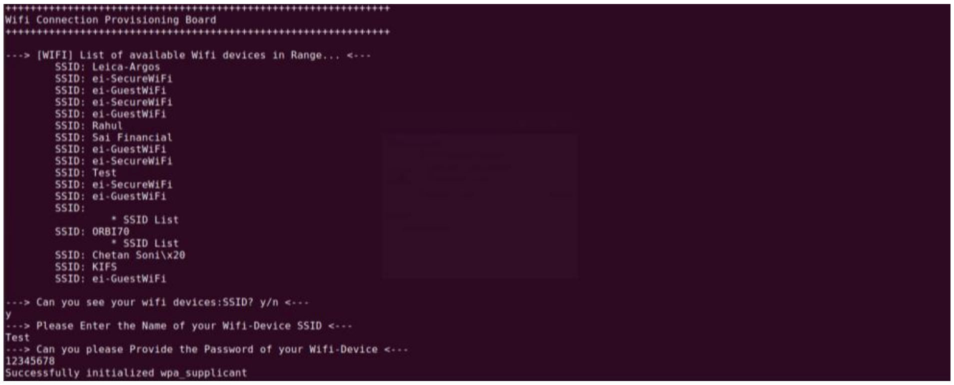
Close window on exit: ○ Always ○ Never ● Only on clean exit

2.2.4 Wi-Fi Setup on the AI_ML Board

1. To connect to a Wi-Fi access point, execute the command from minicom terminal (Linux Host) or Putty (Windows Host) console application as shown below

```
root@imx8qxpaiml:~# ./SSK_Suit_Configuration/wifi_aiml.sh
```

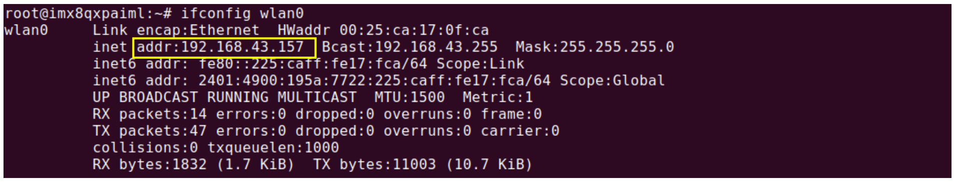
Note - Enter Wi-Fi SSID and Password in the minicom or Putty (Windows Host) console.



```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Wifi Connection Provisioning Board
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

---> [WIFI] List of available Wifi devices in Range... <---
        SSID: Leica-Argos
        SSID: ei-SecureWiFi
        SSID: ei-GuestWiFi
        SSID: ei-SecureWiFi
        SSID: ei-GuestWiFi
        SSID: Rahul
        SSID: Sai Financial
        SSID: ei-GuestWiFi
        SSID: ei-SecureWiFi
        SSID: Test
        SSID: ei-SecureWiFi
        SSID: ei-GuestWiFi
        SSID:
                 * SSID List
        SSID: ORBI70
                 * SSID List
        SSID: Chetan Soni\x20
        SSID: KIFS
        SSID: ei-GuestWiFi

---> Can you see your wifi devices:SSID? y/n <---
y
---> Please Enter the Name of your Wifi-Device SSID <---
Test
---> Can you please Provide the Password of your Wifi-Device <---
12345678
Successfully initialized wpa_supplicant
```

2. Verify the IP address using the command as shown below to ensure that the Linux PC and AI_ML board are in the same network. This is needed during the next steps for copying the data.

```
root@imx8qxpaiml:~# ifconfig wlan0
```



```
root@imx8qxpaiml:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 00:25:ca:17:0f:ca
          inet addr:192.168.43.157  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: fe80::225:caff:fe17:fca/64 Scope:Link
          inet6 addr: 2401:4900:195a:7722:225:caff:fe17:fca/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1832 (1.7 KiB)  TX bytes:11003 (10.7 KiB)
```

2.2.5 File Sharing Setup between Host PC and AI_ML Board

1. For Linux Host PC

   a. File sharing between Linux Host PC and AI_ML board can be performed using Secure Shell Transfer Protocol i.e SCP as shown in below example.

```
Linux_PC:~$ scp root @<AI_ML_IPAddr>:
```

Note – Please note Username (root) Password (root) and IP should be as described in section 2.3.3

2. For Windows Host PC

   a. File sharing between Windows Host PC and AI_ML board can be performed using **Winscp** tool.

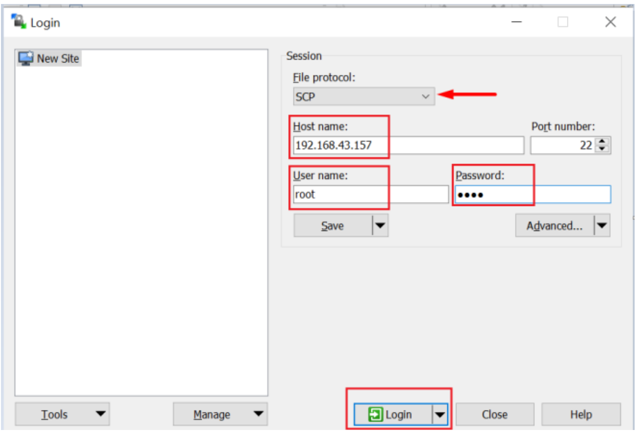
      Note:
      The Winscp tool can be downloaded from the link: https://winscp.net/eng/download.php

   b. Double-click on Winscp icon to start the application.

   c. Please enter board's IP address ("inet addr" noted in yellow above), Username (root) and Password (root-optional) and press "Login" to connect with the AI_ML Board.

Commented [RM1]: Is the password "root-optional"? Or is the password "root", which may be optional?

Commented [KS2R1]: Hello rob,
here password is "root" and an optional input.



File protocol: SCP

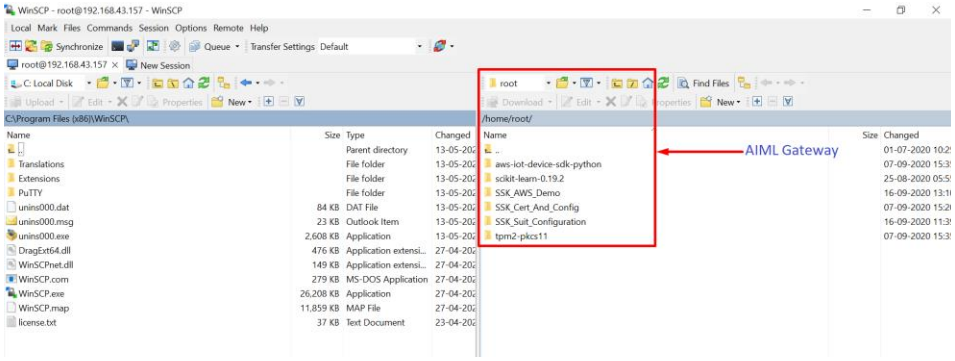
Host name: 192.168.43.157

Port number: 22

User name: root

Password: ••••

   d. Once user is connected to board, the files can be transferred using drag-and-drop feature from left to right pane and vice versa. The left pane should point to the location where the files are stored on the Host PC.



WinSCP - root@192.168.43.157 - WinSCP

root@192.168.43.157

C:\Program Files (x86)\WinSCP\

Name	Size	Type	Changed
..		Parent directory	13-05-202
Translations		File folder	13-05-202
Extensions		File folder	13-05-202
PuTTY		File folder	13-05-202
unins000.dat	84 KB	DAT File	13-05-202
unins000.msg	23 KB	Outlook Item	13-05-202
unins000.exe	2,608 KB	Application	13-05-202
DragExt64.dll	476 KB	Application extensi...	27-04-202
WinSCPnet.dll	149 KB	Application extensi...	27-04-202
WinSCP.com	279 KB	MS-DOS Application	27-04-202
WinSCP.exe	26,208 KB	Application	27-04-202
WinSCP.map	11,859 KB	MAP File	27-04-202
license.txt	37 KB	Text Document	23-04-202

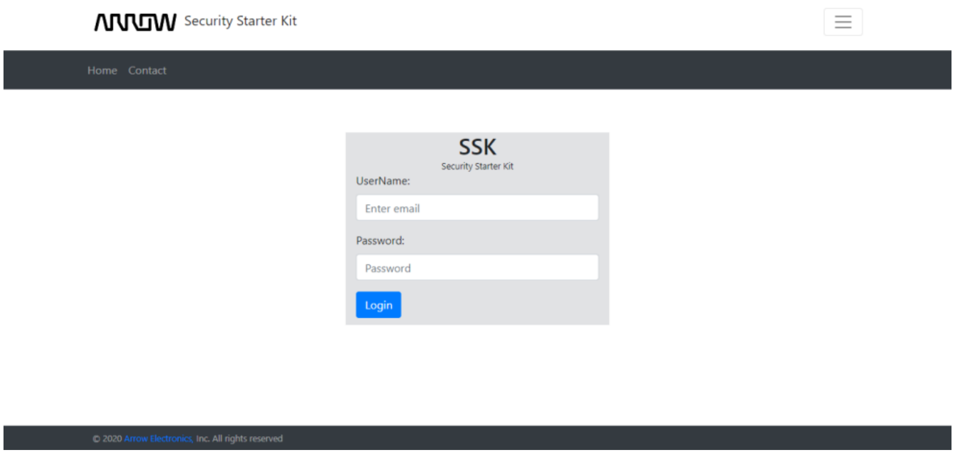
/home/root/

Name	Size	Changed
..		01-07-2020 10:2
aws-iot-device-sdk-python		07-09-2020 15:3
scikit-learn-0.19.2		25-08-2020 05:5
SSK_AWS_Demo		16-09-2020 13:1
SSK_Cert_And_Config		07-09-2020 15:2
SSK_Suit_Configuration		16-09-2020 11:3
tpm2-pkcs11		07-09-2020 15:3

2.3 CA Registration on SSK Cloud Connect

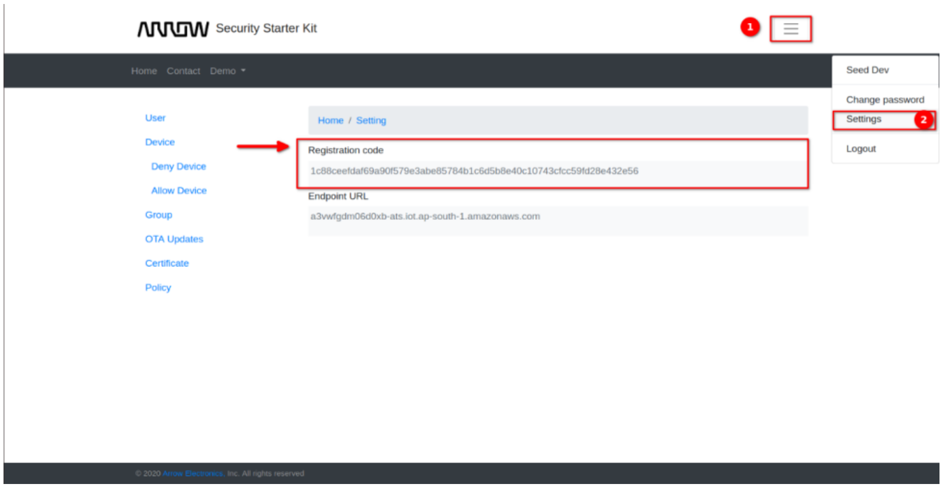
Open the SSK Cloud connect tool using the newly created URL and login credentials for the SSK Cloud Connect EC2 instance, as outlined in section 2.2.1;

1. Login to the SSK Cloud Connect.



2. Register Intermediate ROOTCA with AWS Account

a. User will need AWS Account registration code. To do so, collect from the SSK Cloud Connect >> Option >> Settings >> Registration code.



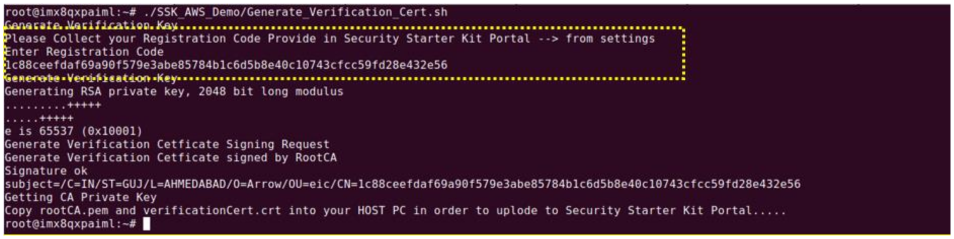
Registration code
1c88ceefdaf69a90f579e3abe85784b1c6d5b8e40c10743cfcc59fd28e432e56

Endpoint URL
a3vwfgdm06d0xb-ats.iot.ap-south-1.amazonaws.com

b. Run the Generate_Verification_Cert.sh script.

```
root@imx8qxpaiml:~# cd /greengrass/certs
root@imx8qxpaiml:~# openssl genrsa -out rootCA.key 2048
root@imx8qxpaiml:~# openssl req -x509 -new -nodes -key rootCA.key -sha256 -days
7000 -out rootCA.pem -subj /C="IN"/ST="GUJ"/L="AHMEDABAD"/O="Arrow"/OU="eic"
root@imx8qxpaiml:~# cd ~/SSK_Suit_Configuration/
root@imx8qxpaiml:~# ./SSK_Suit_Configuration.sh tpm_clear
root@imx8qxpaiml:~# ./SSK_Suit_Configuration.sh
root@imx8qxpaiml:~# cd
root@imx8qxpaiml:~# ./SSK_AWS_Demo/Generate_Verification_Cert.sh
```

c. Script will ask for registration code. Copy the registration code from SSK cloud connect and paste, as shown below:



```
root@imx8qxpaiml:~# ./SSK_AWS_Demo/Generate_Verification_Cert.sh
Generate Verification Key
Please Collect your Registration Code Provide in Security Starter Kit Portal --> from settings
Enter Registration Code
1c88ceefdaf69a90f579e3abe85784b1c6d5b8e40c10743cfcc59fd28e432e56
Generate Verification Key
Generating RSA private key, 2048 bit long modulus
.........+++++
.....+++++
e is 65537 (0x10001)
Generate Verification Cetficate Signing Request
Generate Verification Cetficate signed by RootCA
Signature ok
subject=/C=IN/ST=GUJ/L=AHMEDABAD/O=Arrow/OU=eic/CN=1c88ceefdaf69a90f579e3abe85784b1c6d5b8e40c10743cfcc59fd28e432e56
Getting CA Private Key
Copy rootCA.pem and verificationCert.crt into your HOST PC in order to uplode to Security Starter Kit Portal.....
root@imx8qxpaiml:~#
```

d. Copy "/greengrass/certs/rootCA.pem" and "/greengrass/certs/verificationCert.crt" from AI_ML board to Linux PC or use winscp for Windows Host mentioned in section 2.2.4

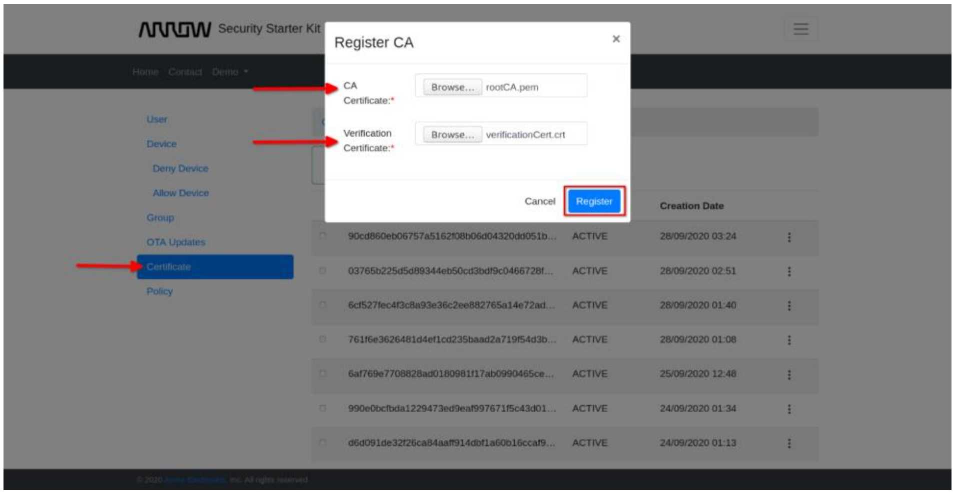
Linux :

```
root@imx8qxpaimh:~# scp /greengrass/certs/rootCA.pem <Linux_PC_usename>@<Linux_PC_IP_Addr>:/PATH
root@imx8qxpaimh:~# scp /greengrass/certs/verificationCert.crt <Linux_PC_usename>@<Linux_PC_IP_Addr>:/PATH
```

Windows :

Use the "WINSCP" tood to copy the files from AI_ML boards to Windows Host PC.

e. Upload the CA certificate (rootCA.pem) and verification certificate (verificationCert.crt), SSK cloud connect >> Certificate >> Register CA on SSK Cloud Connect. This will get the notification "CA Certificate registered successfully".



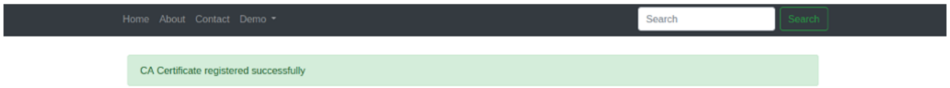
Register CA

CA Certificate:* Browse... rootCA.pem

Verification Certificate:* Browse... verificationCert.crt

Cancel Register

		Creation Date
90cd860eb06757a5162f08b06d04320dd051b...	ACTIVE	28/09/2020 03:24
03765b225d5d89344eb50cd3bdf9c0466728f...	ACTIVE	28/09/2020 02:51
6cf527fec4f3c8a93e36c2ee882765a14e72ad...	ACTIVE	28/09/2020 01:40
761f6e3626481d4ef1cd235baad2a719f54d3b...	ACTIVE	28/09/2020 01:08
6af769e7708828ad0180981f17ab0990465ce...	ACTIVE	25/09/2020 12:48
990e0bcfbda1229473ed9eaf997671f5c43d01...	ACTIVE	24/09/2020 01:34
d6d091de32f26ca84aaff914dbf1a60b16ccaf9...	ACTIVE	24/09/2020 01:13



CA Certificate registered successfully

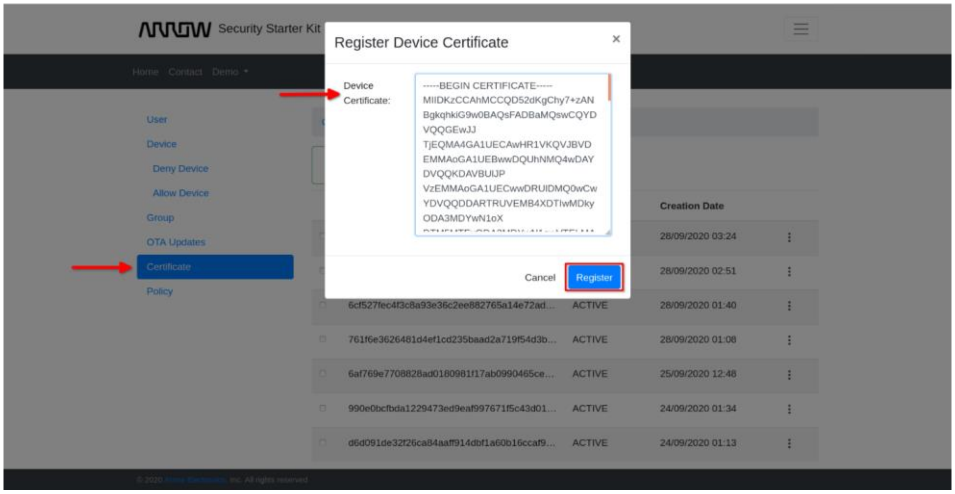
[Note: Please save CA Certificate Number in the Notepad, this will be needed for the next steps]

3. Add OPTIGA™ TPM2.0 Generated Device Certificate to Registered CA

a. Copy the content of Gateway device certificate using below command

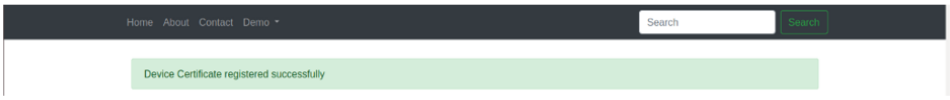
```
root@imx8qxpaimh:~# cat /greengrass/certs/aws_device_cert.pem
                                                  * "-----BEGIN CERTIFICATE-----\n"\
                                                   * "...base64 data...\n"\
                                                   * "-----END CERTIFICATE-----\n"
```

And upload this certificate on SSK Cloud Connect >> Certificate >> Add Certificate >> Select CA certificate (Saved CA number) >> "paste certificate here" >> press, "Register"



```
-----BEGIN CERTIFICATE-----
MIIDKzCCAhMCCQD52dKgChy7+zAN
BgkqhkiG9w0BAQsFADBaMQswCQYD
VQQGEwJJ
TjEQMA4GA1UECAwHR1VKQVJBVD
EMMAoGA1UEBwwDQUhNMQ4wDAY
DVQQKDAVBUlJP
VzEMMAoGA1UECwwDRUlDMQ0wCw
YDVQQDDARTRUVEMB4XDTIwMDky
ODA3MDYwN1oX
```

```
                                              28/09/2020 03:24
                                              28/09/2020 02:51
6cf527fec4f3c8a93e36c2ee882765a14e72ad...  ACTIVE  28/09/2020 01:40
761f6e3626481d4ef1cd235baad2a719f54d3b...  ACTIVE  28/09/2020 01:08
6af769e7708828ad0180981f17ab0990465ce...   ACTIVE  25/09/2020 12:48
990e0bcfbda1229473ed9eaf997671f5c43d01...  ACTIVE  24/09/2020 01:34
d6d091de32f26ca84aaff914dbf1a60b16ccaf9... ACTIVE  24/09/2020 01:13
```



Device Certificate registered successfully

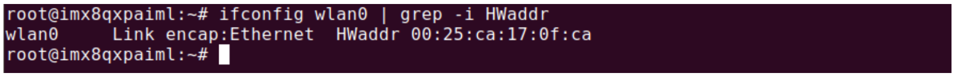
[Note: Please save the newly generated (see the Creation date) Device Certificate Number in the Notepad. This will be needed to attach the certificate to group]

2.4 Demo Setup

2.4.1 AWS Traffic Light Demo configuration and setup

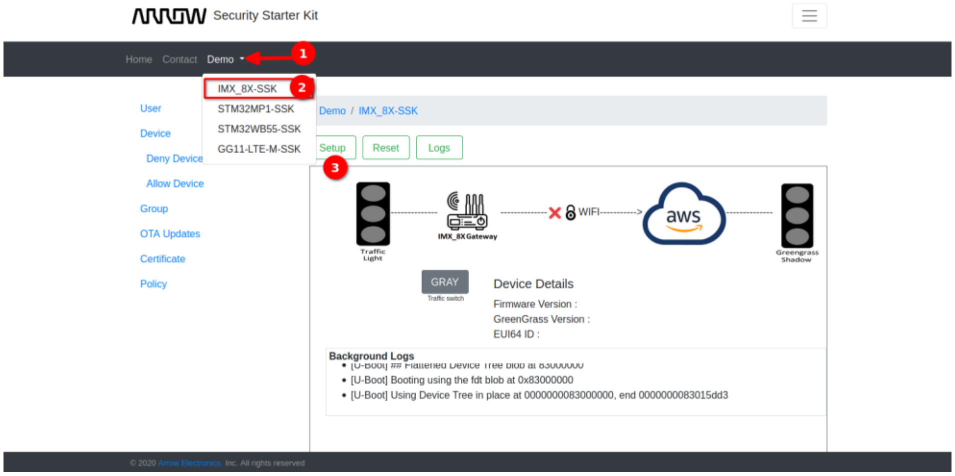
1. Collect the Gateway MAC Address using below command on AI_ML Board using minicom console on Linux PC or putty in case of Windows Host.

```
root@imx8qxpaiml:~# ifconfig wlan0 | grep -i HWaddr
```



```
root@imx8qxpaiml:~# ifconfig wlan0 | grep -i HWaddr
wlan0     Link encap:Ethernet  HWaddr 00:25:ca:17:0f:ca
root@imx8qxpaiml:~# 
```

2. Open the IMX_8X-SSK demo page. Go to SSK Cloud Connect >> Demo >> IMX_8X-SSK
3. Press on "Setup" button.



Device Details

Firmware Version :

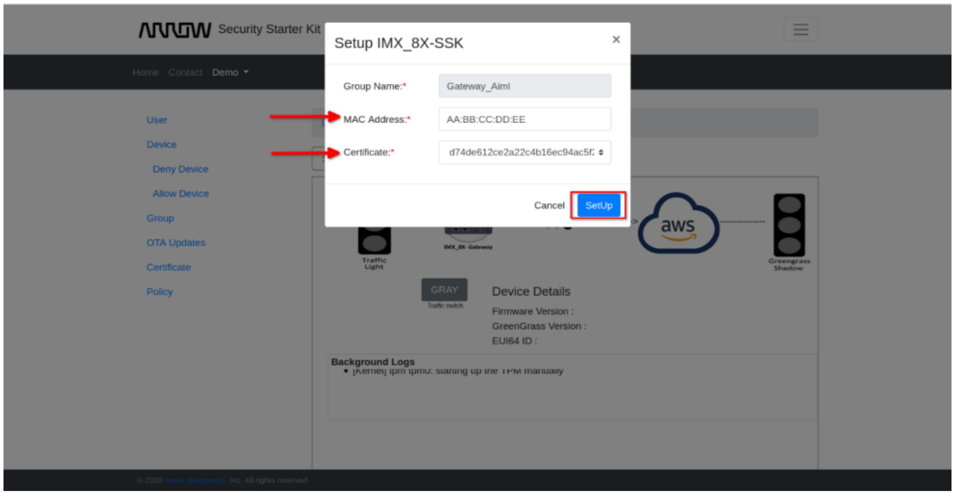
GreenGrass Version :

EUI64 ID :

Background Logs

```
• [U-Boot] ## Flattened Device Tree blob at 83000000
• [U-Boot] Booting using the fdt blob at 0x83000000
• [U-Boot] Using Device Tree in place at 0000000083000000, end 0000000083015dd3
```

4. Enter the MAC address and select Device Certificate (Saved certificate as defined in Section 2.3).
5. Press Click "Setup" button



Setup IMX_8X-SSK

Group Name:* Gateway_Aiml

MAC Address:* AA:BB:CC:DD:EE

Certificate:* d74de612ce2a22c4b16ec94ac5f

Device Details

Firmware Version :

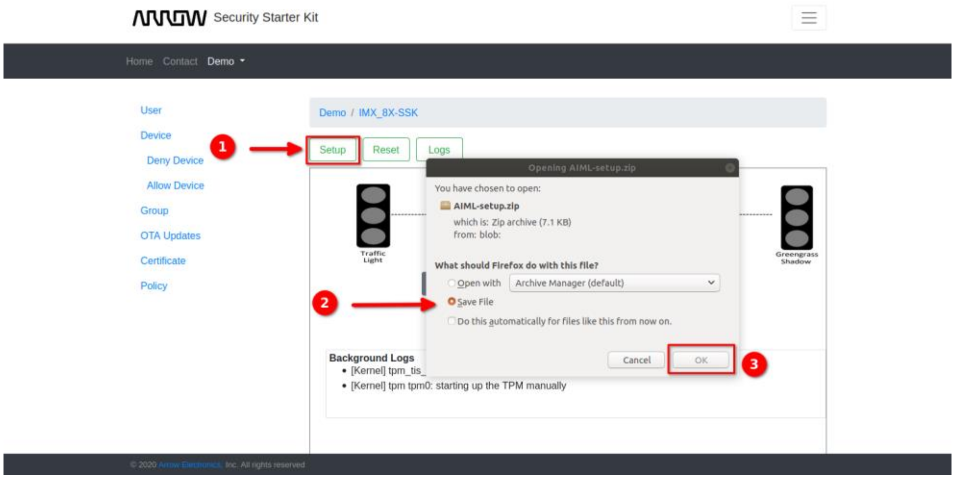
GreenGrass Version :

EUI64 ID :

Background Logs

```
• [Kernel] tpm tpm0: starting up the TPM manually
```

6. See the dialog window as shown below, and download the AIML-setup.zip file.



Opening AIML-setup.zip

You have chosen to open:

AIML-setup.zip

which is: Zip archive (7.1 KB)
from: blob:

What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

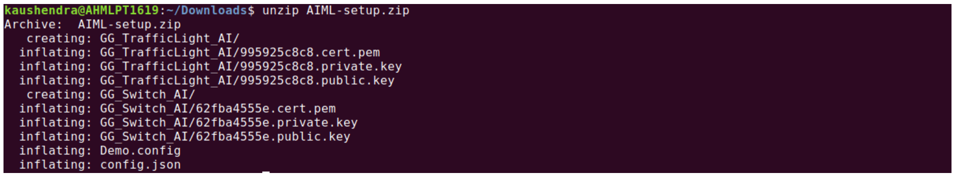
□ Do this automatically for files like this from now on.

Background Logs

- [Kernel] tpm_tis_
- [Kernel] tpm tpm0: starting up the TPM manually

- Unzip using Linux

```
Linux_PC:~$ unzip AIML-setup.zip
```



```
kaushendra@AHMLPT1619:~/Downloads$ unzip AIML-setup.zip
Archive:  AIML-setup.zip
   creating: GG_TrafficLight_AI/
  inflating: GG_TrafficLight_AI/995925c8c8.cert.pem
  inflating: GG_TrafficLight_AI/995925c8c8.private.key
  inflating: GG_TrafficLight_AI/995925c8c8.public.key
   creating: GG_Switch_AI/
  inflating: GG_Switch_AI/62fba4555e.cert.pem
  inflating: GG_Switch_AI/62fba4555e.private.key
  inflating: GG_Switch_AI/62fba4555e.public.key
  inflating: Demo.config
  inflating: config.json
```

- Unzip using Windows

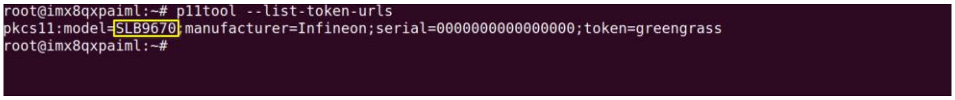
  Use Winzip or another favorite tool

7. You will need to check the OPTIGA™ TPM 2.0 silicon soldered in your kit, using the command below. This information is required in the next step.

```
root@stm32mp1-av96:~# p11tool --list-token-urls
```

<u>Note:</u> Difference in the silicon part number prefix

- SLB (Commercial Temp grade)
- SLM (Industrial Temp grade)



```
root@imx8qxpaiml:~# p11tool --list-token-urls
pkcs11:model=SLB9670;manufacturer=Infineon;serial=0000000000000000;token=greengrass
root@imx8qxpaiml:~#
```

8. Edit the config.json file with the appropriate silicon that was provided in step #7. This file will be found in the directory you recently created when unzipping the AI ML-setup.zip; /IoT Greengrass/config/config.json

   Note: The user can use the following methods to edit the file;

   1. From the Windows command prompt, type: notepad **config.json** and make the change shown below
   2. The "vi" command is referenced and used below, but you can use any Editor to perform the same function.

```
root@imx8qxpaiml:~# vi /greengrass/config/config.json

"principals": {
     "IoTCertificate": {
       "privateKeyPath":
"pkcs11:model=SLB9670;manufacturer=Infineon;token=greengrass;object=greenkey;type=privat
e;pin-valu;
       "certificatePath": "file:///greengrass/certs/aws_device_cert.pem"
     }
   },
```

9. Zip file contains the GG_Trafic_Light_AI and GG_Switch_AI certificates and key, user needs to copy all the files to AI_ML board as mentioned below using commands or use winscp for Windows Host mentioned in section 2.2.4:

Linux:

```
Linux_PC:~$ scp GG_TrafficLight_AI/* root@<AI_ML_IPAddr>:/home/root/SSK_AWS_Demo/
Linux_PC:~$ scp GG_Switch_AI/* root@<AI_ML_IPAddr>:/home/root/SSK_AWS_Demo/
Linux_PC:~$ scp Demo.config root@<AI_ML_IPAddr>:/home/root/SSK_AWS_Demo/
Linux_PC:~$ scp config.json root@<AI_ML_IPAddr>:/greengrass/config/
```

Windows:

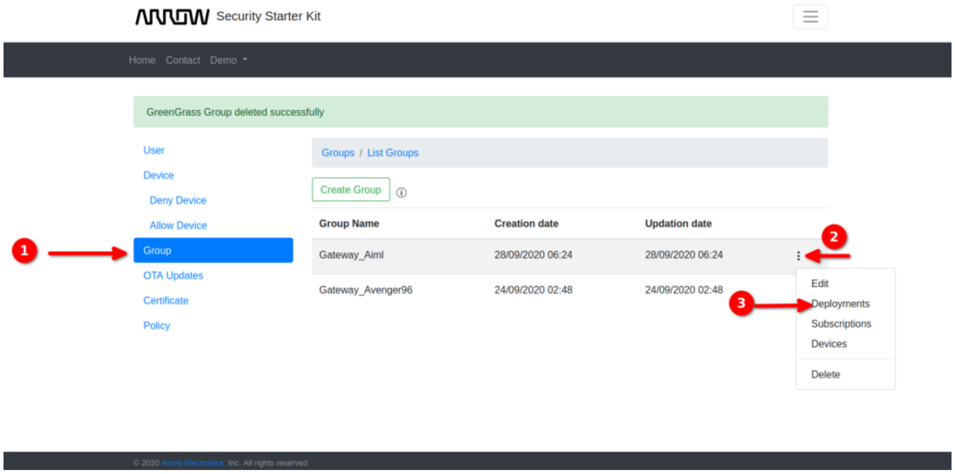
1. Use the "WINSCP" tool to copy ONLY the files contained in the directory (not the entire directory) from the GG_TrafficLight and GG_Switch directories on the Windows Host PC to AI_ML Board directory here; SSK_AWS_Demo.
2. Use the "WINSCP" tool to copy the files; Demo.config and config.json to the SSE_AWS_Demo directory on the AI_ML board.

2.4.2 Deploying Greengrass Group

1. Run the Greengrass demo on AI_ML board using command as shown below before the deployment process

```
root@imx8qxpaiml:~#/greengrass/ggc/core/greengrassd start
```

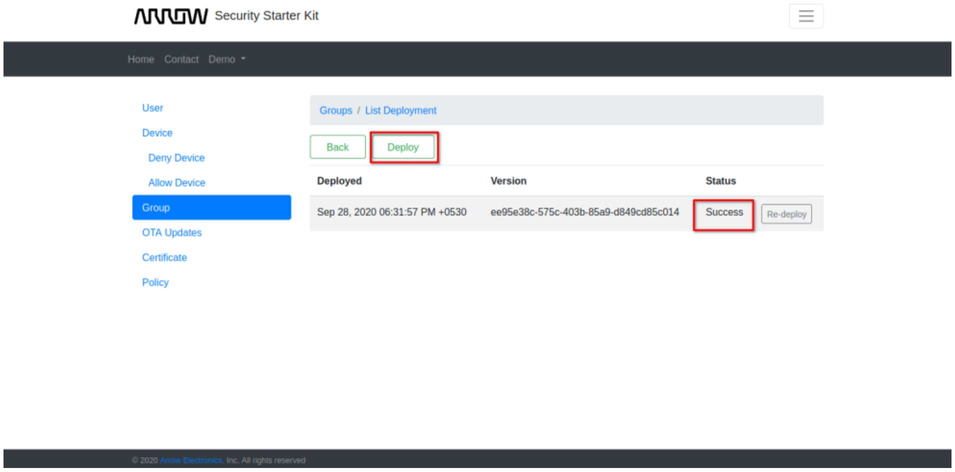
2. Go to SSK Cloud Connect >> Group >> Gateway_Aiml >> Deployments , choose Deploy Option Provided



GreenGrass Group deleted successfully

Group Name	Creation date	Updation date
Gateway_Aiml	28/09/2020 06:24	28/09/2020 06:24
Gateway_Avenger96	24/09/2020 02:48	24/09/2020 02:48

3. After successful deployment of AWS IoT Greengrass, user will get update status of deployment process as shown below



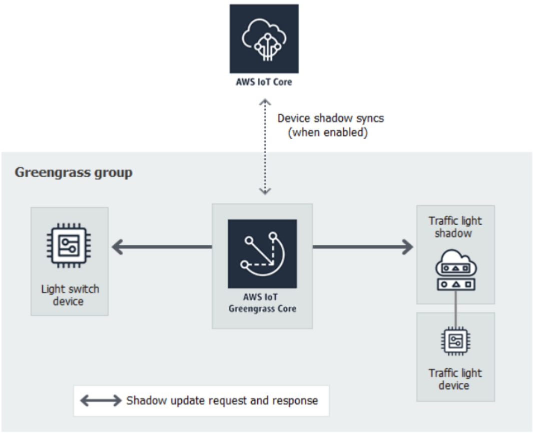
Deployed	Version	Status
Sep 28, 2020 06:31:57 PM +0530	ee95e38c-575c-403b-85a9-d849cd85c014	Success

Setup completed on SSK Cloud Connect for AWS Traffic Light Demo

2.4.3 Run AWS Traffic Light Demo

This demo shows how a AWS IoT Greengrass enabled device can interact with AWS IoT device shadows in an AWS IoT Greengrass group [Gateway_Aiml]. A Greengrass shadow is a JSON document that is used to store current or desired state information for devices.

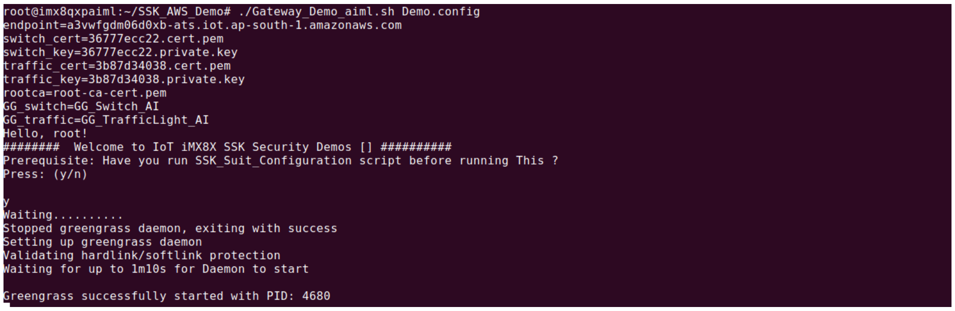
In this demo, one can observe how one AWS IoT Greengrass device [GG_Switch_AI] can modify the state of another AWS IoT Greengrass device [GG_TrafficLight_AI] and how these states can be synced to the AWS Cloud:



- Run the Demo script on the AI_ML Board

```
root@imx8qxpaiml:~# cd SSK_AWS_Demo
root@imx8qxpaiml:~# ./Gateway_Demo_aiml.sh Demo.config
```

Note: When prompted for (y/n), type "y"

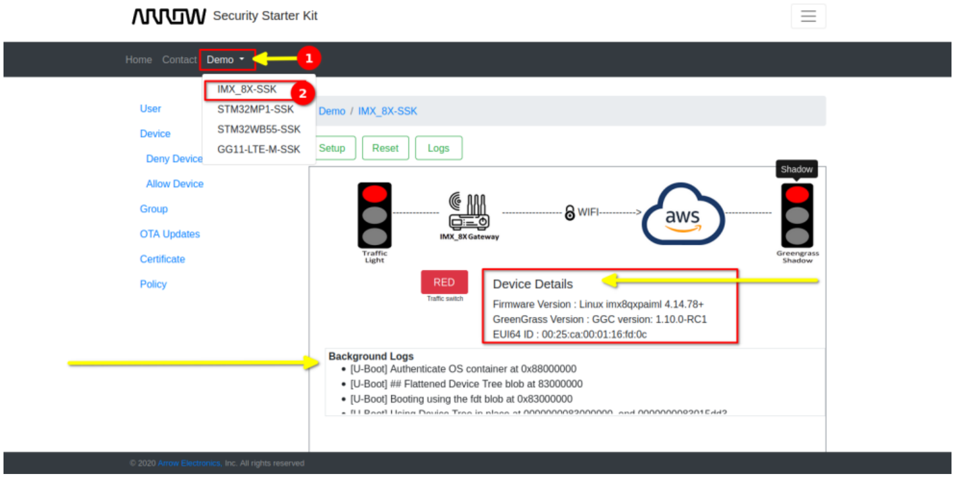


```
root@imx8qxpaiml:~/SSK_AWS_Demo# ./Gateway_Demo_aiml.sh Demo.config
endpoint=a3vwfgdm06d0xb-ats.iot.ap-south-1.amazonaws.com
switch_cert=36777ecc22.cert.pem
switch_key=36777ecc22.private.key
traffic_cert=3b87d34038.cert.pem
traffic_key=3b87d34038.private.key
rootca=root-ca-cert.pem
GG_switch=GG_Switch_AI
GG_traffic=GG_TrafficLight_AI
Hello, root!
########  Welcome to IoT iMX8X SSK Security Demos [] ##########
Prerequisite: Have you run SSK_Suit_Configuration script before running This ?
Press: (y/n)

y
Waiting..........
Stopped greengrass daemon, exiting with success
Setting up greengrass daemon
Validating hardlink/softlink protection
Waiting for up to 1m10s for Daemon to start

Greengrass successfully started with PID: 4680
```

2.4.4 Demo Result

SSK Cloud Connect >> Demo >> IMX_8X-SSK

- On SSK Cloud Connect dashboard, the Traffic Light indication changed from Green to Yellow to Red according to Traffic switch condition.
- On the right side, the shadow of the traffic light signal displays the same color as indicated on Amazon cloud. AI_ML board sends the traffic signals to the cloud securely, using the hardware security chip - OPTIGA™ TPM 2.0.
- Device Details – AI_ML board sends the current firmware version, Greengrass version, EUI64 ID to AWS cloud and displays the same on the Dashboard.
- Background Logs – Displays the secure boot, U-Boot, Kernel and OPTIGA™ TPM 2.0 messages on dashboard and are continuously scrolled.



Device Details

Firmware Version : Linux imx8qxpaiml 4.14.78+

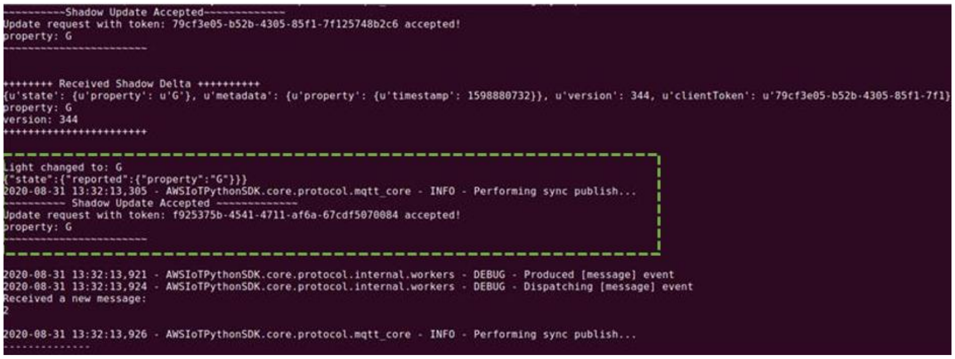
GreenGrass Version : GGC version: 1.10.0-RC1

EUI64 ID : 00:25:ca:00:01:16:fd:0c

Background Logs

- [U-Boot] Authenticate OS container at 0x88000000
- [U-Boot] ## Flattened Device Tree blob at 83000000
- [U-Boot] Booting using the fdt blob at 0x83000000

- On AI_ML board, User can see the Traffic light indication logs, as shown below:

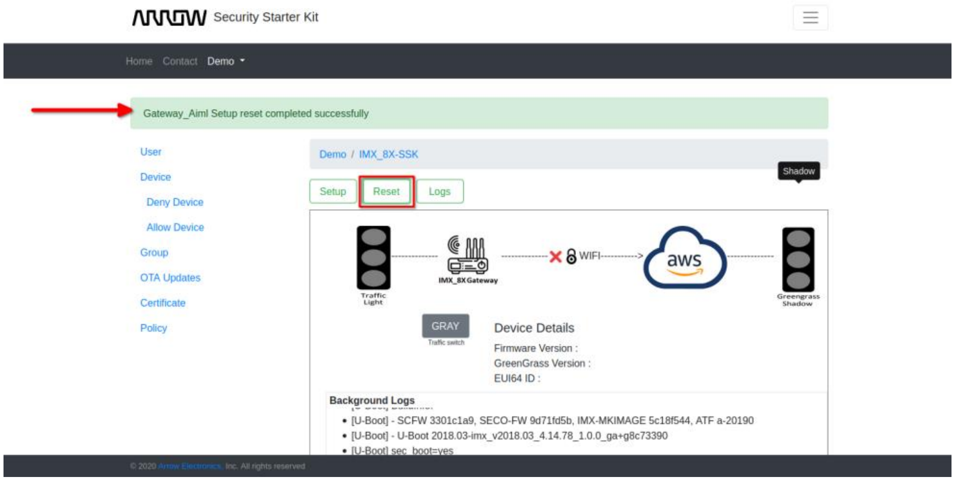


```
-----------Shadow Update Accepted-------------
Update request with token: 79cf3e05-b52b-4305-85f1-7f125748b2c6 accepted!
property: G
----------------------


++++++++ Received Shadow Delta ++++++++++
{u'state': {u'property': u'G'}, u'metadata': {u'property': {u'timestamp': 1598880732}}, u'version': 344, u'clientToken': u'79cf3e05-b52b-4305-85f1-7f1}
property: G
version: 344
++++++++++++++++++++++

Light changed to: G
{"state":{"reported":{"property":"G"}}}
2020-08-31 13:32:13,305 - AWSIoTPythonSDK.core.protocol.mqtt_core - INFO - Performing sync publish...
---------- Shadow Update Accepted -------------
Update request with token: f925375b-4541-4711-af6a-67cdf5070084 accepted!
property: G
----------------------

2020-08-31 13:32:13,921 - AWSIoTPythonSDK.core.protocol.internal.workers - DEBUG - Produced [message] event
2020-08-31 13:32:13,924 - AWSIoTPythonSDK.core.protocol.internal.workers - DEBUG - Dispatching [message] event
Received a new message:
2

2020-08-31 13:32:13,926 - AWSIoTPythonSDK.core.protocol.mqtt_core - INFO - Performing sync publish...
-------------
```

- If a user wants to reset the setup follow SSK Cloud Connect >> Demo >> IMX_8X-SSK >> Press "Reset" button

- Kill the demo process (or by pressing "CRTL + C") and reboot the AI_ML board, using below command.

```
root@imx8qxpaiml:~# reboot –f
```



Gateway_Aiml Setup reset completed successfully

Device Details

Firmware Version :

GreenGrass Version :

EUI64 ID :

Background Logs

- [U-Boot] - SCFW 3301c1a9, SECO-FW 9d71fd5b, IMX-MKIMAGE 5c18f544, ATF a-20190
- [U-Boot] - U-Boot 2018.03-imx_v2018.03_4.14.78_1.0.0_ga+g8c73390
- [U-Boot] sec_boot=yes

© 2020 Arrow Electronics, Inc. All rights reserved

2.4.5 Demo Inference

Security Stater kit with I.MX 8X and OPTIGA™ TPM 2.0 demo covers the below listed functionalities:

1. **AWS Provisioning** – Secure AWS Device Provisioning using OPTIGA™ TPM 2.0 chip to securely store the Gateway Device Certificate and Keys.
2. **AWS Authentication** – Secure OPTIGA™ TPM 2.0 chip stores the Gateway Device Certificate, which is authenticated with AWS Intermediate ROOTCA.
3. **Secure Communication** – Using OPTIGA™ TPM 2.0 to stores the session credentials, secure communication between AWS and the AI_ML board is established. .
4. **AWS Greengrass** – Enabled AWS Greengrass features on the AI_ML gateway for device Shadow Service.
5. **Secure Boot** – Enabled secure boot features on AI_ML Gateway Board.
6. **Measure boot** – Using OPTIGA™ TPM 2.0, Gateway is verifying the boot sequence.

Note: For more details about all above functionalities, please refer the following documents, located here; https://www.arrow.com/en/products/imx-8x-ssk/arrow-development-tools

- i.MX_8X-SSK Developers Guide.pdf
- Security Starter Kit Cloud Quick Start Guide.pdf
- Security Starter Kit Cloud Connect Installation & Setup Guide.pdf
- Security Starter Kit Cloud Connect Users Guide.pdf