Quick Start Guide

Security Starter Kit with STM32MP157 and OPTIGA™ TPM 2.0

Date: March 03, 2021 | Version 1.2

CONTENTS

DEFINITION, ACRONYMS AND ABBREVIATIONS

Definition/Acronym/Abbreviation	Description
AV96	Avenger96 Board (with STM32MP157CAC MPU installed)
AWS	Amazon Web Services
CA	Certificate Authority
GG	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 Security Starter Kit with STM32MP157 and OPTIGA™ TPM 2.0 will provide AWS IoT Greengrass Demo running on the Avenger96 using the Infineon OPTIGA™ TPM 2.0 (Infineon SLB9670 or SLM9670). This demo showcases the security features and functionality of provisioning, authentication, and secure communication between the STM32MP157 and the Cloud via WiFi with AWS IoT Greengrass.

1.2 Prerequisite

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

- Security Starter Kit Setup will require following
  - Arrow 96boards Avenger96 SBC (with the STM32MP157CAC3 MPU installed)
  - Arrow 96boards Tresor Mezzanine card (with the OPTIGA™ TPM 2.0 installed)
  - SDcard – 16GB
  - MicroUSB debug cable
  - Autec WM24P6-12-A-QL Power Supply
- Linux PC with Minicom OR Windows PC with Putty
- Internet connectivity (Wi-Fi/Ethernet) of Board and Host PC should be on same Network.

1.3 Scope of Detailed Design

The integration of AWS IoT Greengrass with STM32MP157 & OPTIGA™ TPM 2.0 to provide a secure, hardware-based gateway/edge compute device. This integration ensures the use of private key to establish device identity, which is securely stored in tamper-proof hardware devices. These features prevent the device from being compromised, impersonated, and other malicious activities.

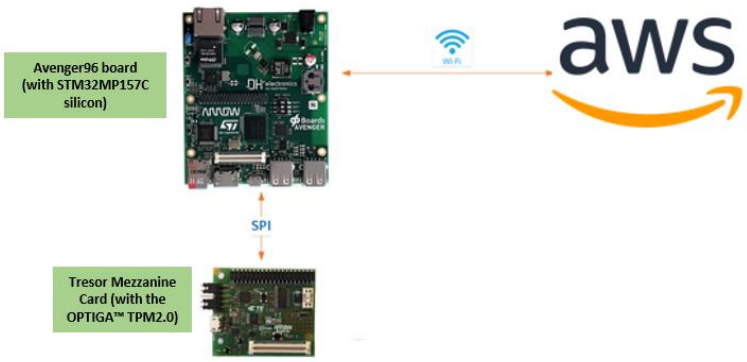


Figure 1: Hardware Configuration

2 INSTALLATION STEPS

2.1 Hardware setup - Security Starter Kit with STM32MP1 and OPTIGA™ TPM 2.0

The STM32MP1 board is shipped from the factory, pre-configured with the proper S3 Dip Switch settings and SD Card pre-installed. If this is not a new board out of the box, please confirm the proper hardware setup in the STM32MP157-SSK Developers Guide.pdf Section 3.1 for the Hardware Setup details. https://www.arrow.com/en/products/stm32mp157-ssk/arrow-development-tools

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

The mezzanine will be mounted on top of the Avenger96 board as shown in Figure 2. When the Avenger96 board is powered-up, the Power LED on the OPTIGA™ TPM2.0 board turns on, indicating that the board is correctly connected.

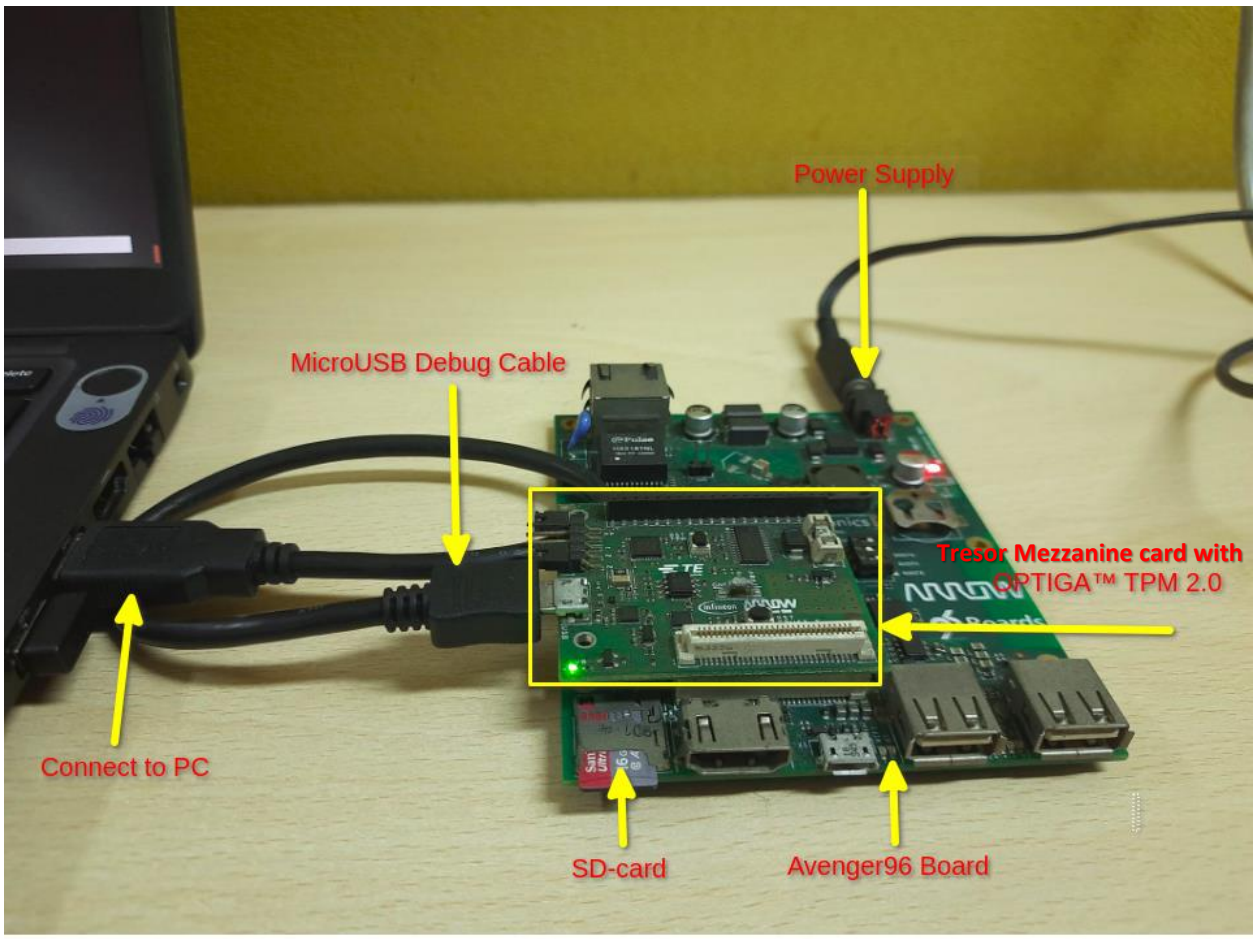


Figure 2: Hardware Setup

2.2 Software setup – Security Starter Kit with STM32MP1 and OPTIGA™ TPM 2.0

2.2.1 AWS Account creation and Arrow Cloud Connect tool configuration

The items mentioned below are specific to enabling AWS Cloud Services with the Security Starter Kit and only need to be completed 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, you will need 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 will need to 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
   Linked here: https://www.arrow.com/en/products/stm32wb55-ssk/arrow-development-tools

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

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

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

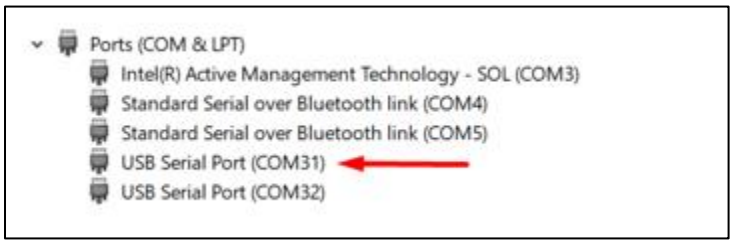
3. Set baud rate and other setting to the below values
   a. Baud rate 115200
   b. Parity none
   c. hardware flow control/software flow control none
   d. Serial device /dev/ttyUSB0
   e. **save setup as dfl**

4. After the Avenger96 board boots up, it will display the login console in the minicom terminal on the Linux PC.
5. Username for board is “root” without any password (if asked for)

```
Avenger96 v3.3 - ST OpenSTLinux - Weston - (A Yocto Project Based Distro) 2.6-snapshot stm32mp1-av96 ttySTM0
stm32mp1-av96 login: root (automatic login)

root@stm32mp1-av96:~#
```

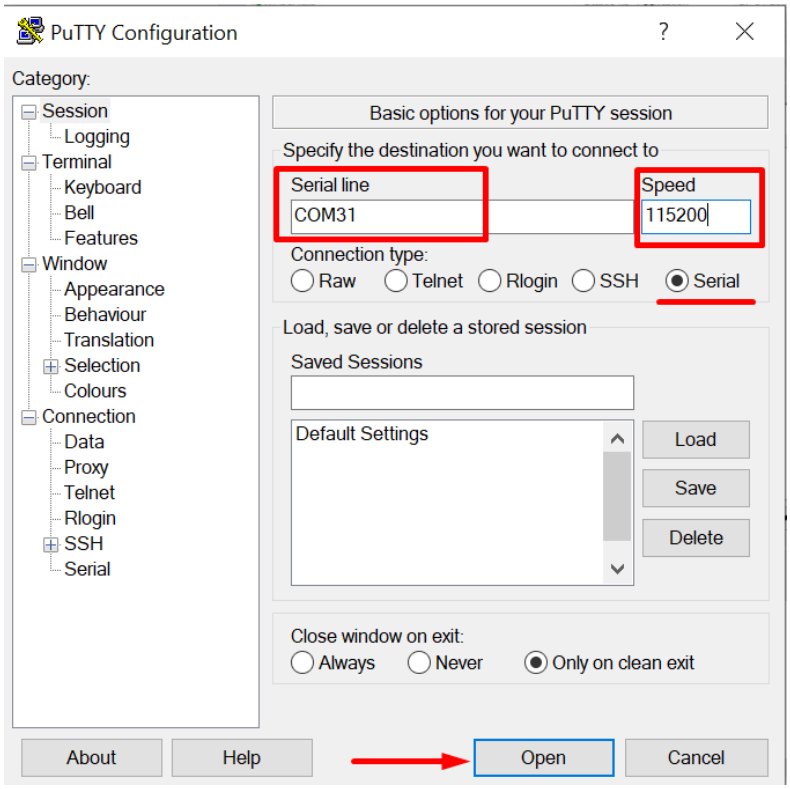
2.2.3 Software Setup on Windows Host PC (For Windows Users)

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



3. Open the 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.



2.2.4 Wi-Fi Setup Avenger96 Board

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

Note: Once the terminal window opens, if you don't see a command line then hit enter.

```
root@stm32mp1-av96:~# ./SSK_Suit_Configuration/wifi_avg.sh
```

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

```
root@stm32mp1-av96:~# ./SSK_Suit_Configuration/wifi_avg.sh
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
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 of the board using the below command to ensure that the Host PC and Avenger96 board are in the same network. This is needed in next steps for copying data.

```
root@stm32mp1-av96:~# ifconfig wlan0
```

```
root@stm32mp1-av96:~# ifconfig wlan0
wlan0     Link encap:Ethernet  HWaddr 10:98:C3:64:CD:8A
          inet addr:192.168.43.107  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2405:205:c946:743d:1298:c3ff:fe64:cd8a/64 Scope:Global
          inet6 addr: fe80::1298:c3ff:fe64:cd8a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1924 (1.8 KiB)  TX bytes:14993 (14.6 KiB)
```

```
Linux_Host@dell:~$ scp  root@<Avg96_IPAddr>:
```

Note:

- The <Avg96_IPAddr> required in the command line, is shown next to "inet addr" in the screen above (section 2.2.4, step 2). Please use the Username (root) Password (root)

2. For Windows Host PC

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

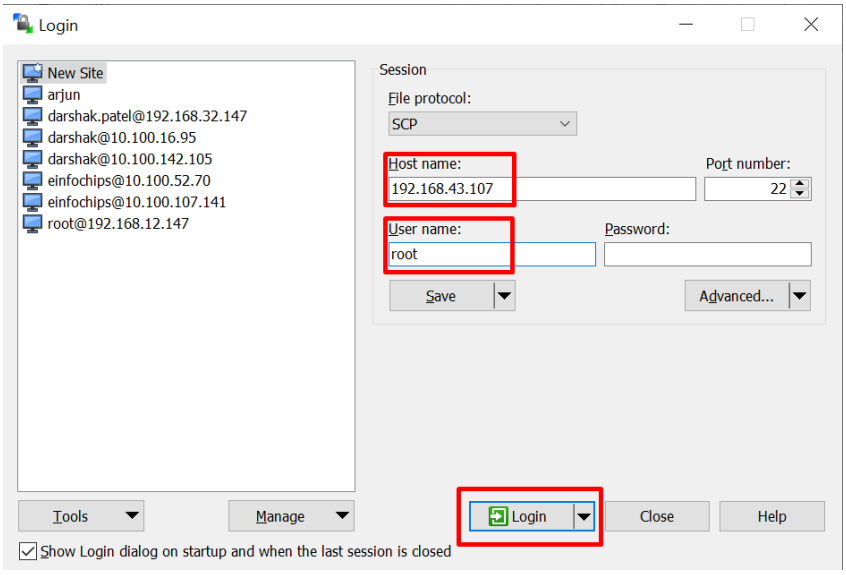
Note:

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

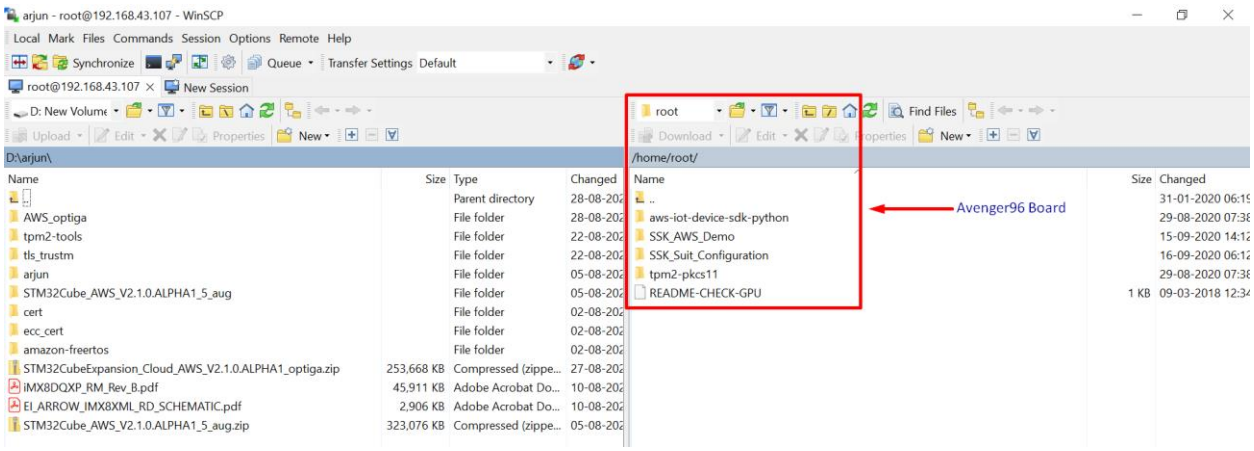
b. Double-click on the Winscp icon to start the application.

c. Please enter board's IP address ("inet addr" notated in yellow above, Section 2.2.4, step 2), Username (root) and Password (root) and press "Login" to connect with the Avenger96 Board.

Note: The password (root) may be optional depending on your host PC configuration. If the credentials are not accepted using the password, try again with no password.



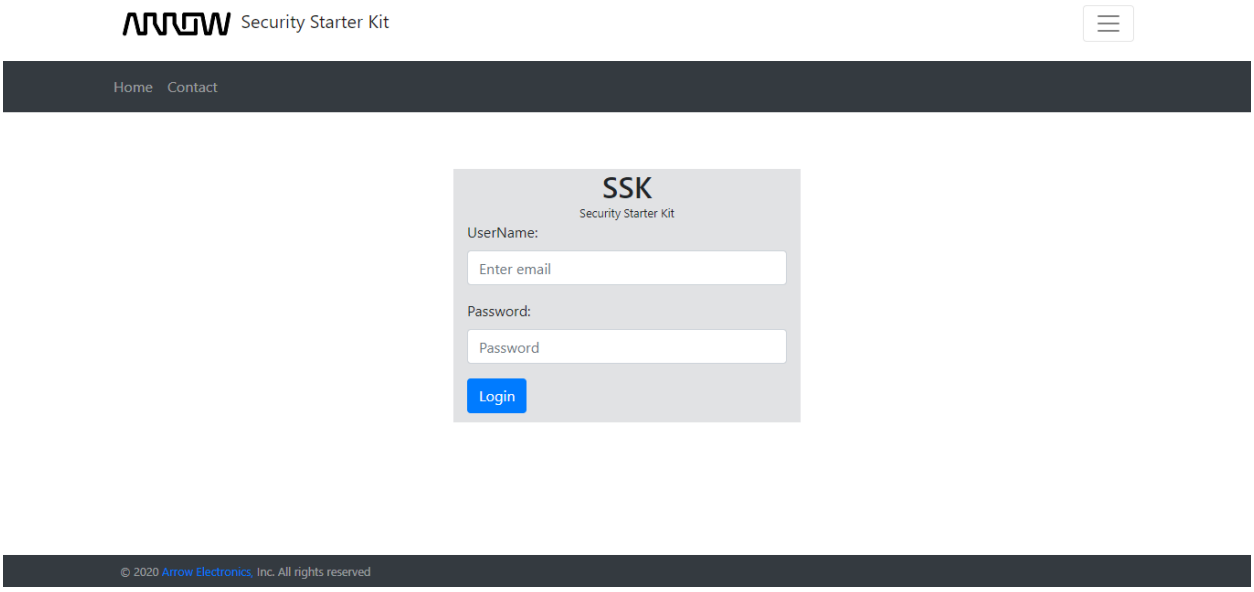
d. Once WinSCP is connected to the board, the files can be transferred using drag-and-drop from the left to right pane or vice versa.



2.3 CA Registration on SSK Cloud Connect

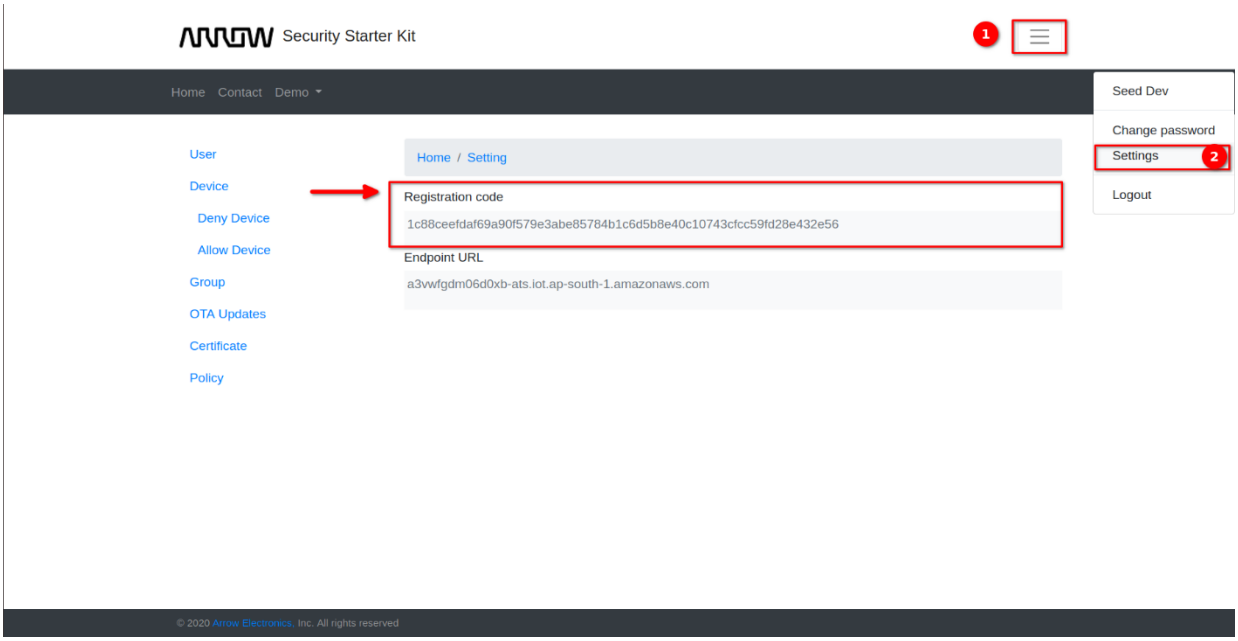
Open the SSK Cloud connect tool using the newly created URL and login credentials for the SSK Cloud Connect EC2 instance, as outlined in section 2.2.1:

1. Login to the SSK Cloud Connect Provided with your AWS Active Credentials.



2. Register Intermediate ROOTCA with AWS Account

   a. User will need your AWS Account registration code. To find it, navigate from the SSK Cloud Connect >> Option (Burger) >> Settings >> Registration code.



b. Run the Generate_Verification_Cert.sh script on the AV96 board.

```
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. The script will ask for your registration code, please copy the registration code from SSK cloud connect and paste it as shown below:

```
root@stm32mp1-av96:~# ./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 (2 primes)
.....................+++++
.........+++++
e is 65537 (0x010001)
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 SECUITY-STARTER-KIT Portal.....
root@stm32mp1-av96:~#
```

d. Copy "/greengrass/certs/rootCA.pem" and "/greengrass/certs/verificationCert.crt" from the Avenger96 board to the Linux PC or use winscp for a Windows Host as mentioned in section 2.2.4

Linux:

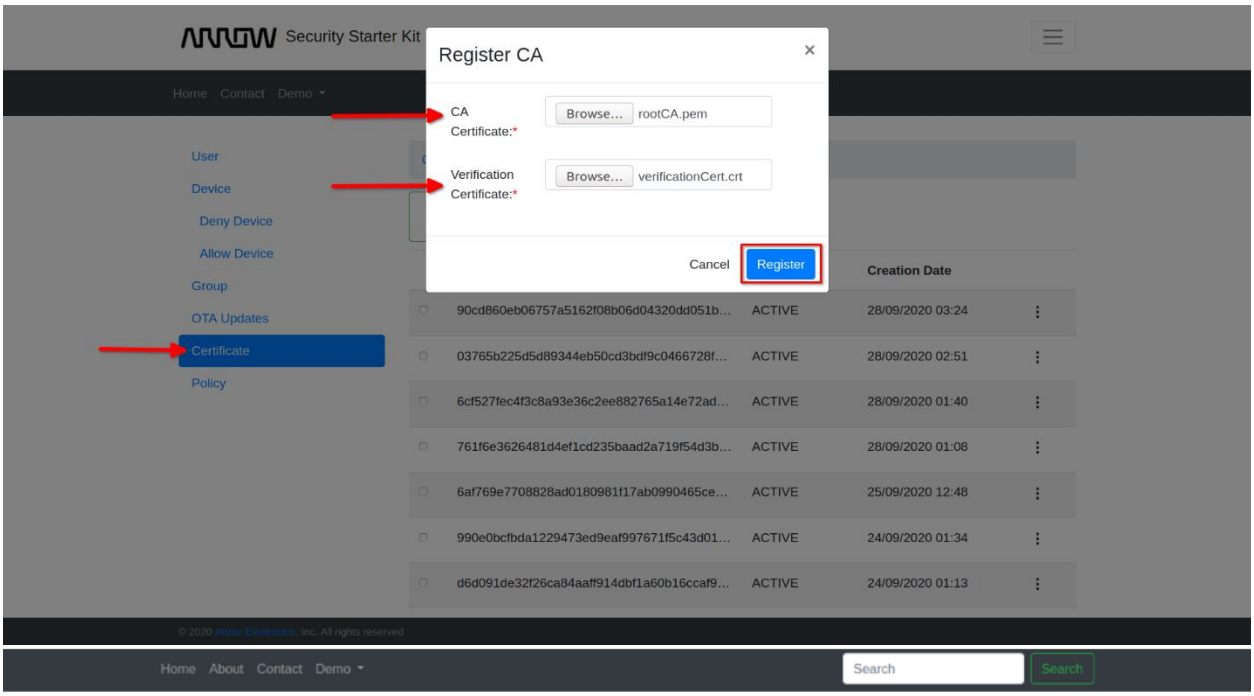
```
root@stm32mp1-av96:~# scp /greengrass/certs/rootCA.pem  <Linux_PC_usename>@<Linux_PC_IP_Addr>:/PATH
root@stm32mp1-av96:~# scp /greengrass/certs/verificationCert.crt  <Linux_PC_usename>@<Linux_PC_IP_Addr>:/PATH
```

Windows:

Use the "WINSCP" tool to copy the files from Avenger96 boards to Windows host PC.

e. Upload the CA certificate (rootCA.pem) and verification certificate (verificationCert.crt) to the SSK Cloud Connect instance. Upload these in the path: SSK cloud connect >> Certificate >> Register CA on SSK Cloud Connect. Once uploaded you should get the notification "CA Certificate registered successfully".

Note: This step may produce an "error" but will continue to function properly. This error is typically due to the board CA certificate having been previously uploaded and registered.



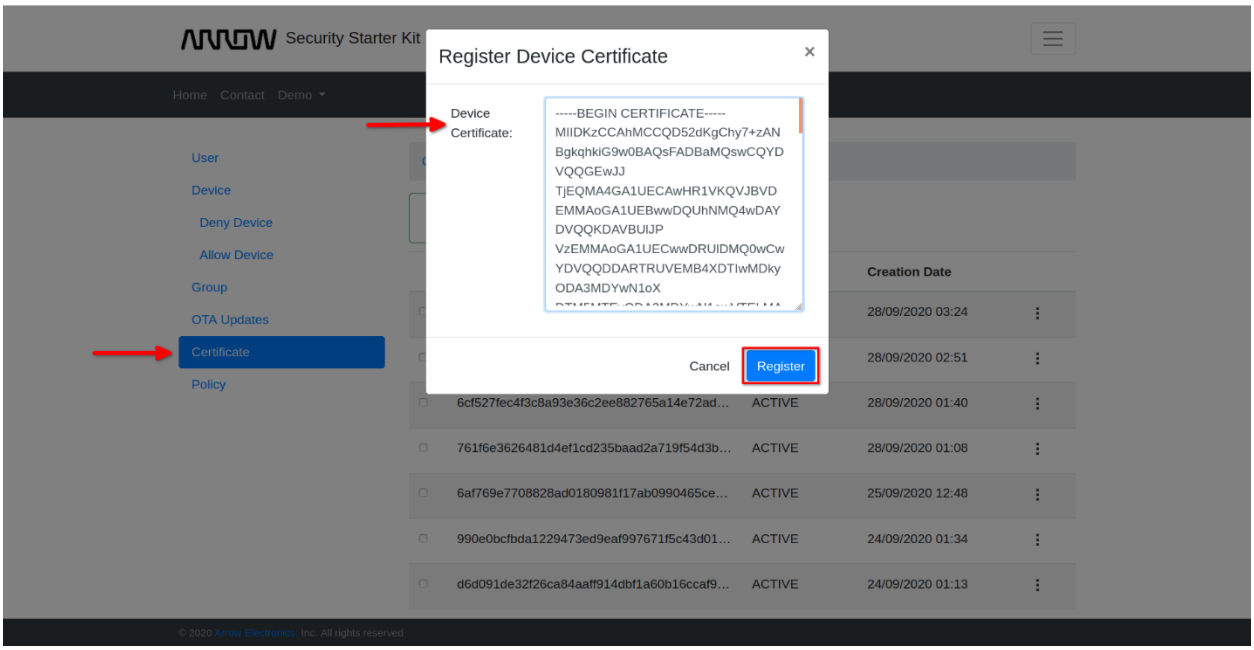
[Note: Please save the CA Certificate Number in a Notepad, this will be needed for the next steps]

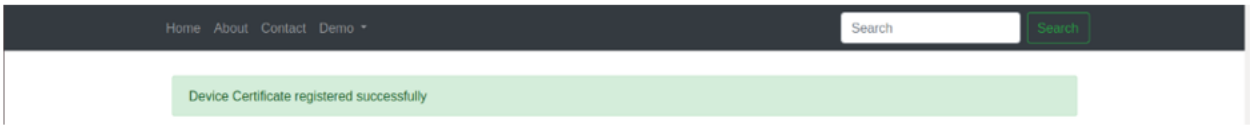
3. Add OPTIGA™ TPM 2.0 Generated Device Certificate to Registered CA

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

```
root@stm32mp1-av96:~# 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”





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

2.4 Demo Setup

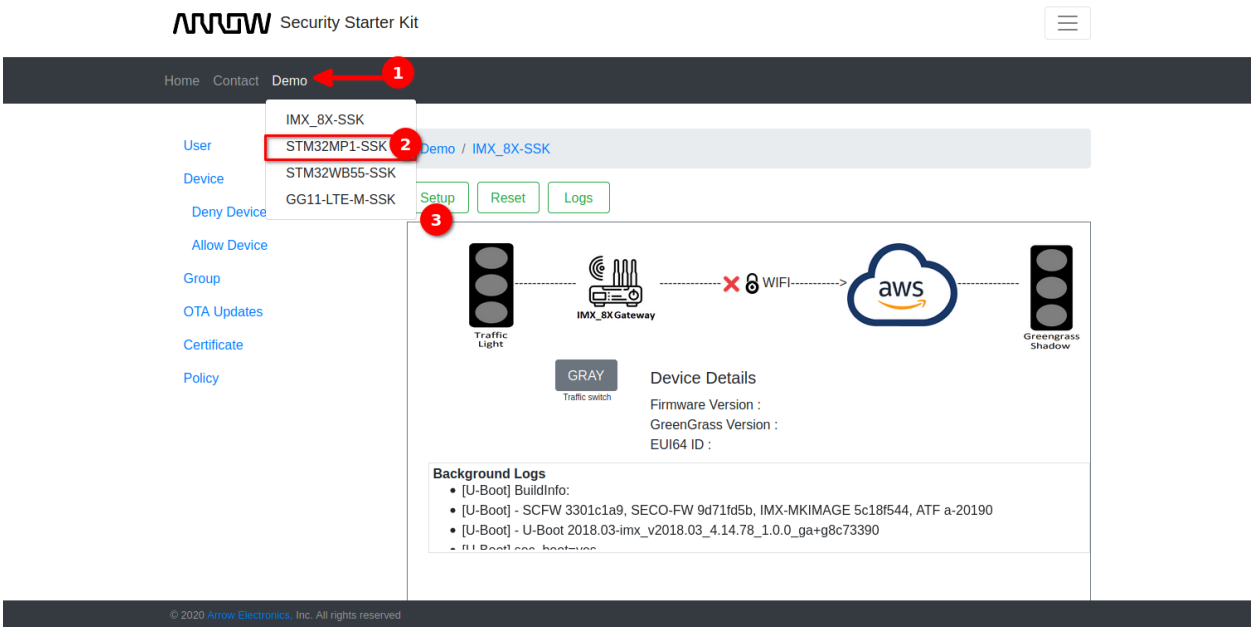
2.4.1 AWS Traffic Light Demo configuration

1. Collect the Gateway MAC Address using below command on Avenger96 Board using Minicom console on a Linux PC or Putty for a Windows Host.

```
root@stm32mp1-av96:~# ifconfig wlan0 | grep -i HWaddr
```

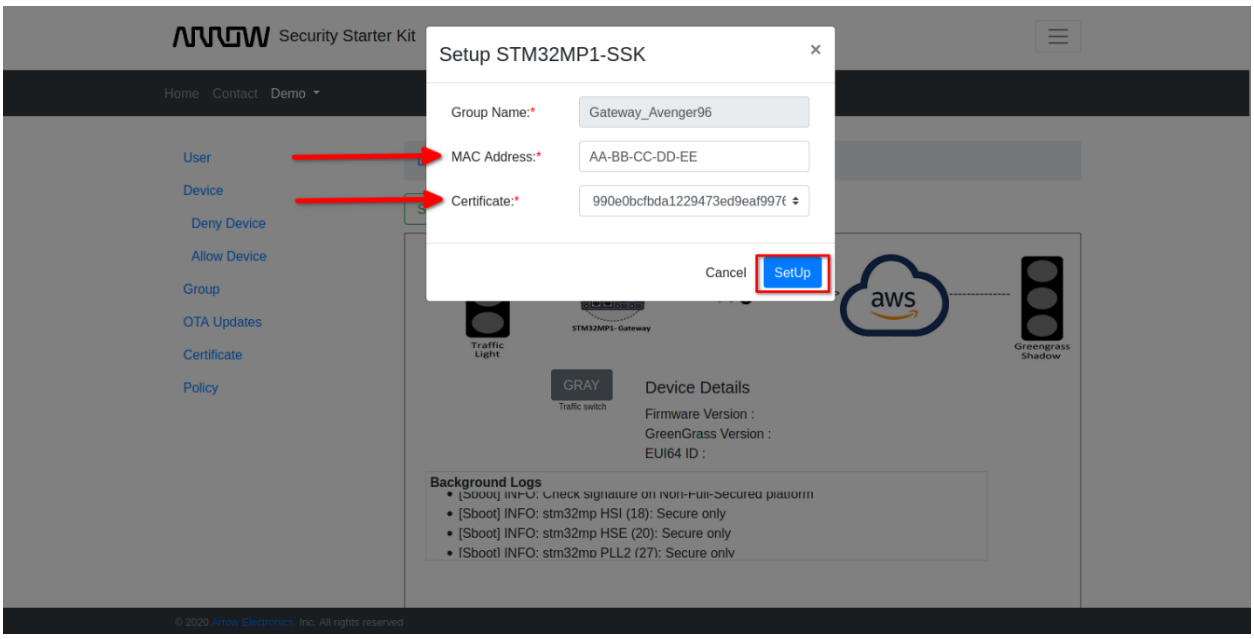
```
root@stm32mp1-av96:~# ifconfig wlan0 | grep -i HWaddr
wlan0     Link encap:Ethernet  HWaddr 10:98:C3:64:CD:8A
```

2. Open the STM32MP1-SSK demo page. Go to SSK Cloud Connect >> Demo >> STM32MP1-SSK
3. Press the “Setup” button.

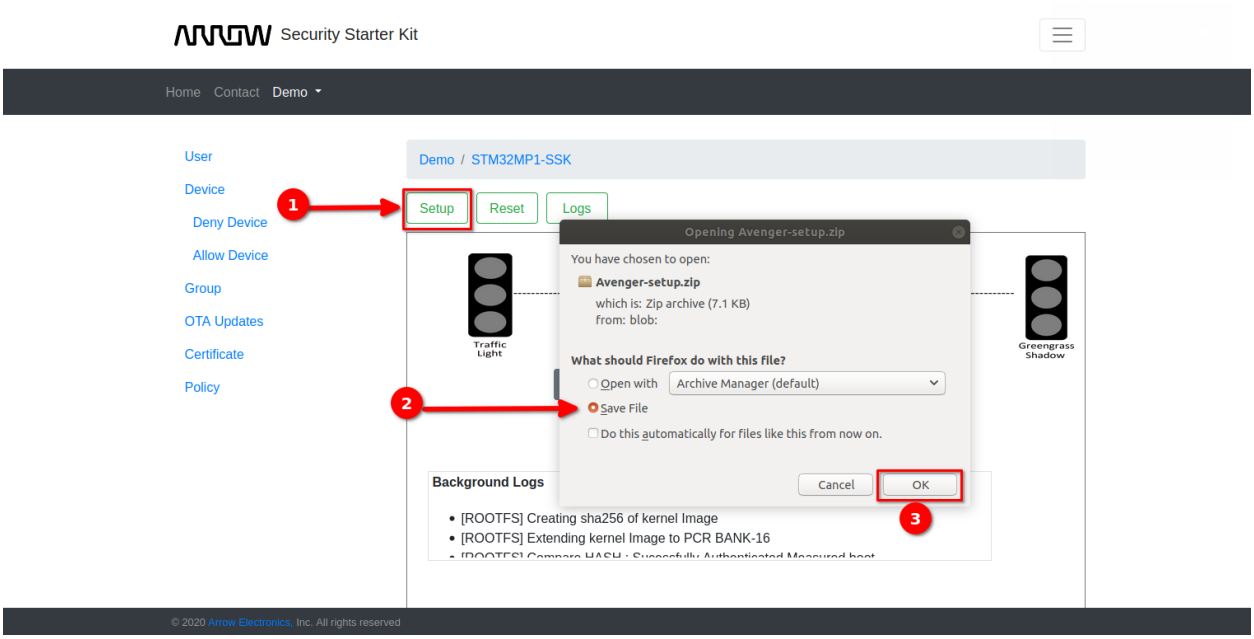


4. Enter the MAC address and paste in the selected Device Certificate (Saved certificate is defined in Section 2.3).

5. Press “Setup” button



6. Please see the dialog window below, and download the Avenger-setup.zip file as indicated:



- Unzip within Linux

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

```
kaushendra@AHMLPT1619:~/Downloads$ unzip Avenger-setup.zip
Archive:  Avenger-setup.zip
   creating: GG_TrafficLight/
  inflating: GG_TrafficLight/8341f52128.cert.pem
  inflating: GG_TrafficLight/8341f52128.private.key
  inflating: GG_TrafficLight/8341f52128.public.key
   creating: GG_Switch/
  inflating: GG_Switch/4fee4f0e47.cert.pem
  inflating: GG_Switch/4fee4f0e47.private.key
  inflating: GG_Switch/4fee4f0e47.public.key
  inflating: Demo.config
  inflating: config.json
```

- Unzip within Windows
  Use Winzip or another preferred 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
```

Note: There are different silicon part number prefixes

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

```
root@stm32mp1-av96:~# p11tool --list-token-urls
pkcs11:model=SLB9670;manufacturer=Infineon;serial=0000000000000000;token=greengrass
root@stm32mp1-av96:~#
```

8. Edit the config.json file with the appropriate silicon that was discovered above in step #7. This file will be found in the directory you recently created when unzipping the Avenger-setup.zip: /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 show below. Or open and edit with any text editor of your choice.
   2. For Linux the "vi" command is referenced and used below, but you can use any Editor to perform the same function.

```
root@stm32mp1-av96:~# vi /greengrass/config/config.json

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

9. The unzipped file contains the GG_Trafic_Light and GG_Switch certificates and key. The user needs to copy all the files to the Avenger96 board using the below commands or using winscp for Windows Host mentioned in section 2.2.4:

Linux:

```
Linux_PC:~$ scp GG_TrafficLight/*   root@<AV96_IPAddr>:/home/root/SSK_AWS_Demo/
Linux_PC:~$ scp GG_Switch/*   root@< AV96_IPAddr>:/home/root/SSK_AWS_Demo/
Linux_PC:~$ scp Demo.config   root@< AV96_IPAddr>:/home/root/SSK_AWS_Demo/
Linux_PC:~$ scp config.json   root@< AV96_IPAddr>:/greengrass/config/
```

Windows:

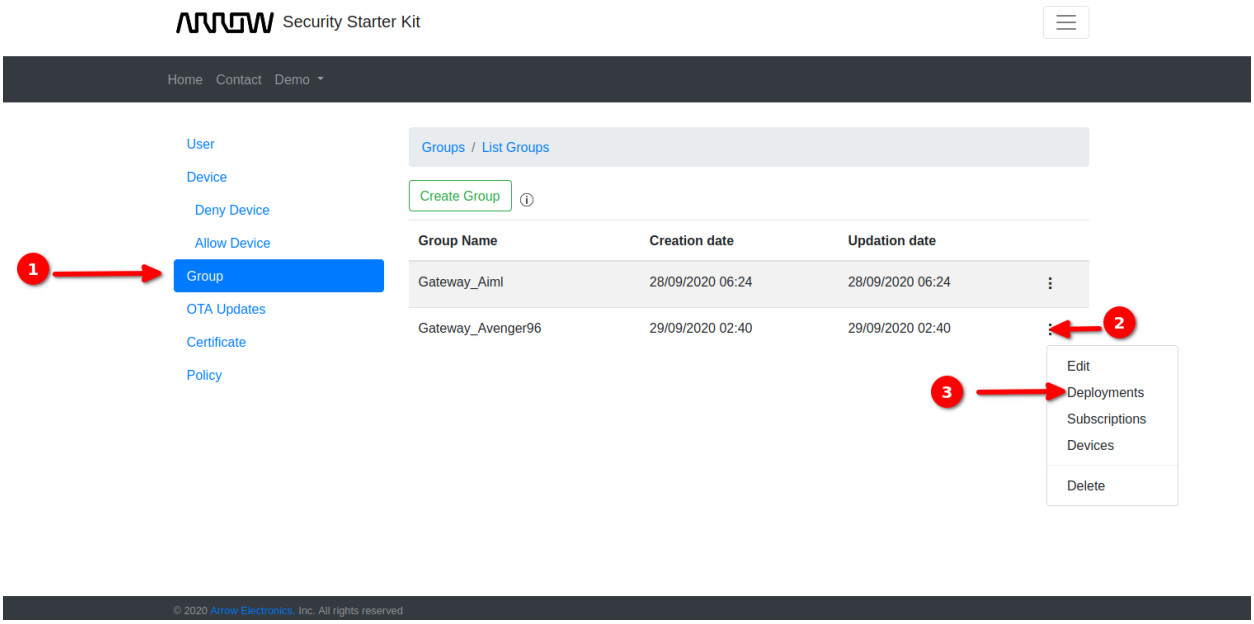
1. Use the "WINSCP" tool to copy ONLY the files contained in the directory (not the entire directory) from the GG_TrafficLight and GG_Switch directories on the Windows host PC to Avenger96 Board directory here: /home/root/SSK_AWS_Demo/
2. Use the "WINSCP" tool to copy the files: Demo.config and config.json to the SSE_AWS_Demo directory on the Avenger96 board.

2.4.2 Deploying IoT Greengrass Group

1. Run the IoT Greengrass demo on the AV96 STM32MP157-SSK board using the command below, before moving to the next step.

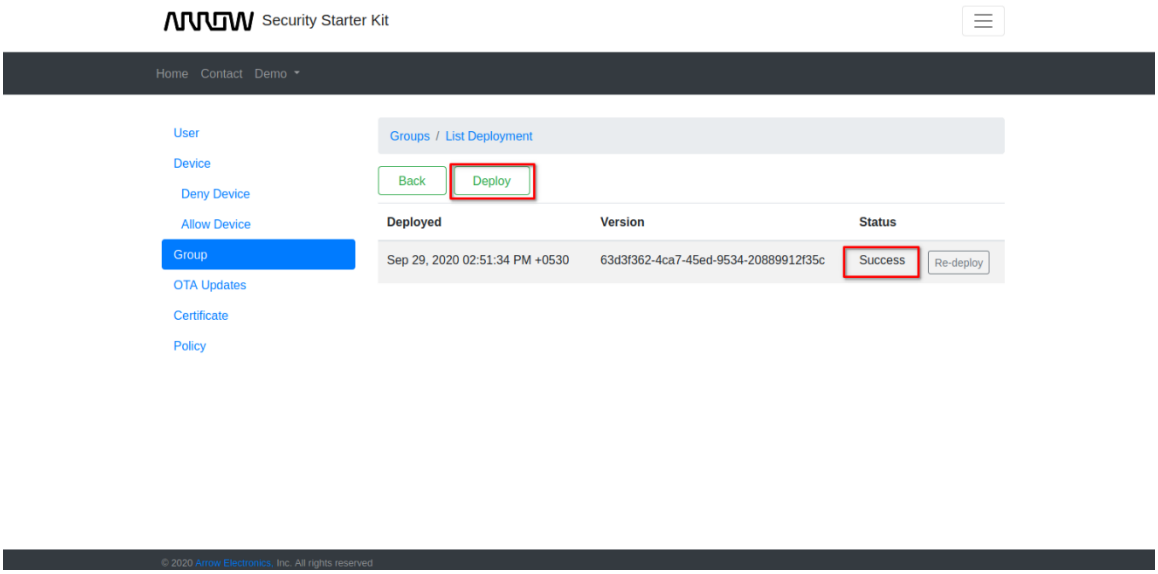
```
root@stm32mp1-av96:~# cd /greengrass/ggc/core/
root@stm32mp1-av96:~#./greengrassd start
```

2. Go to SSK Cloud Connect >> Group >> Gateway_Avenger96 >> Deployments, choose the Deploy Option



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

   Note: You may need to refresh your page to see the changes.

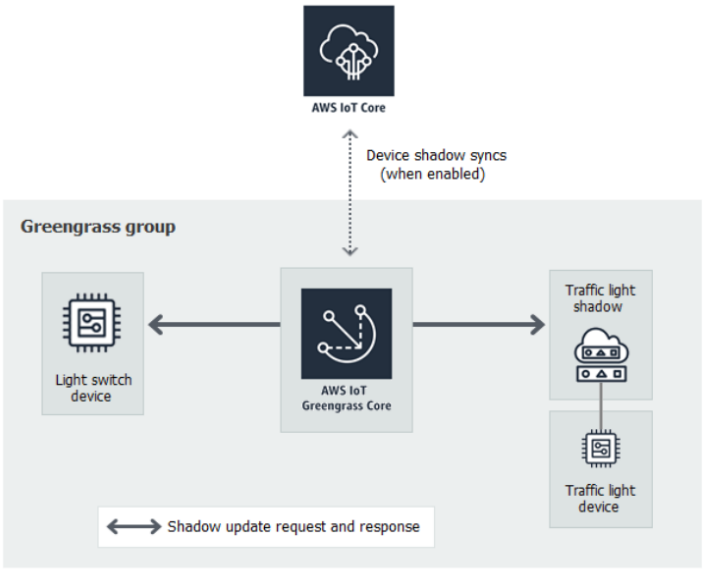


Setup completed on SSK Cloud Connect for AWS Traffic Light Demo

2.4.3 Run AWS Traffic Light Demo

This demo shows how an AWS IoT Greengrass enabled device can interact with an IoT Connected device and shadows in an AWS IoT Greengrass group [Gateway_Avenger96]. An IoT Greengrass shadow is a JSON document that is used to store current or desired state information for devices.

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



- Run the Demo script on the Avenger96 Board,

```
root@stm32mp1-av96:~# cd SSK_AWS_Demo
root@stm32mp1-av96:~# ./Gateway_Demo_avg.sh Demo.config
```

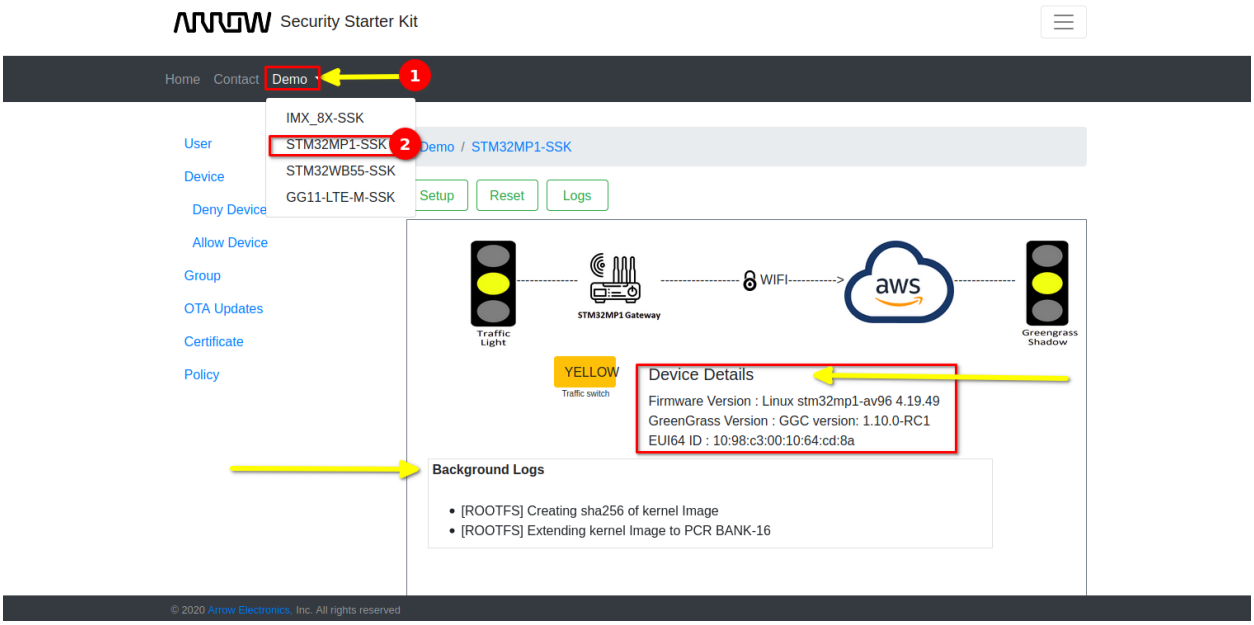
Note: When prompted for (y/n), type “y”

```
root@stm32mp1-av96:~/SSK_AWS_Demo# ./Gateway_Demo_avg.sh Demo.config
endpoint=a3vwfgdm06d0xb-ats.iot.ap-south-1.amazonaws.com
switch_cert=73225c8fd5.cert.pem
switch_key=73225c8fd5.private.key
traffic_cert=c714a851ba.cert.pem
traffic_key=c714a851ba.private.key
rootca=root-ca-cert.pem
GG_switch=GG_Switch
GG_traffic=GG_TrafficLight
Hello, root!
########  Welcome to STM32MP1 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: 9777
```

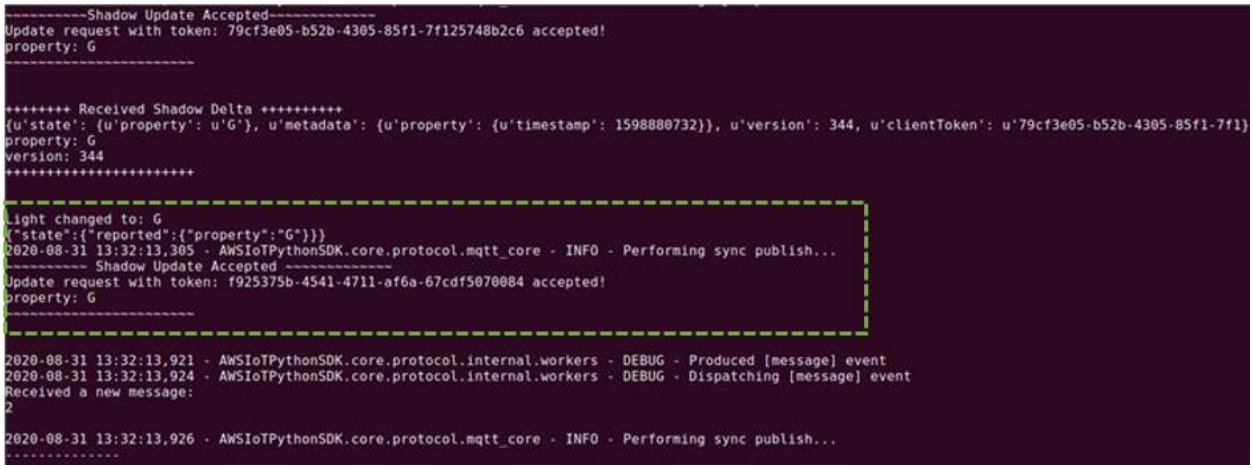
2.4.4 Demo Result

SSK Cloud Connect >> Demo >> STM32MP1-SSK

- On the SSK Cloud Connect dashboard, Traffic Light indication changed from Green to Yellow to Red according to Traffic switch condition.
- On the right Side, a shadow of the traffic light signal is displayed with the same color as indicated on AWS. Avenger96 board is sending the traffic signals to cloud securely using hardware a security chip - OPTIGA™ TPM 2.0.
- Device Details – Avenger96 board sends the current firmware version, IoT Greengrass version, EUI64 ID to AWS cloud and displays the same on the Dashboard.
- Background Logs – Displays the secure boot, UBoot, Kernel and OPTIGA™ TPM 2.0 messages on dashboard and continuously scrolls



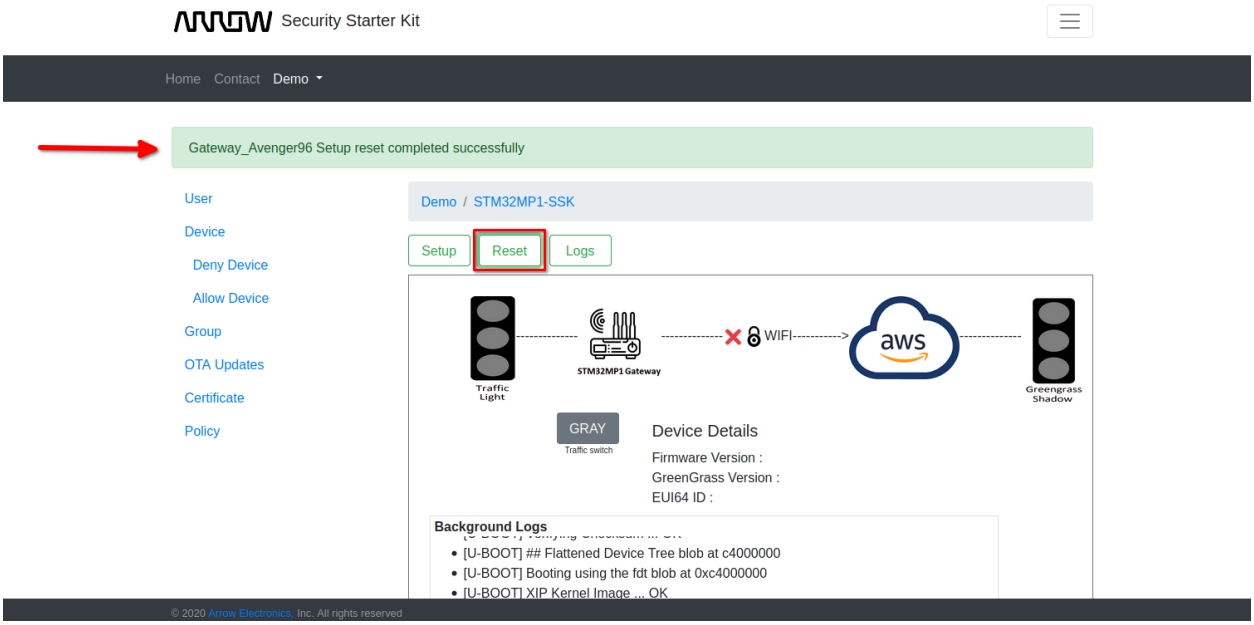
- On Avenger96 board, User can see the Traffic light indication logs, as shown below:



- If a user wants to reset the Setup
  Please follow SSK Cloud Connect >> Demo >> STM32MP1-SSK >> Press “Reset” button

- Kill the demo process (or by pressing “CRTL + C”) and reboot the Avenger96 board, using below command.

```
root@stm32mp1-av96:~# reboot -f
```



2.4.5 Demo Inference

The AV96 Security Stater kit with STM32MP1 and OPTIGA™ TPM 2.0 Demo provides an example and showcases 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 securely communicates between AWS and Avenger96 gateway by storing the session credentials.
4. AWS IoT Greengrass – Enabled AWS IoT Greengrass feature in the Avenger96 gateway for device Shadow Service.
5. Secure Boot – Enabled secure boot features on the Avenger96 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/stm32mp157-ssk/arrow-development-tools

- STM32MP157-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