

Quick Start Guide

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

Date: November 5, 2020 | Version 1.0
FINAL



The Solutions People



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	17
2.4.4	Demo Result	18
2.4.5	Demo Inference	20

DEFINITION, ACRONYMS AND ABBREVIATIONS

Definition/Acronym/Abbreviation	Description
AI_ML board	Arrow 96boards I.IMX8X_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™ TPM 2.0 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™ TPM 2.0 installed)
 - SDcard – 16GB
 - MicroUSB debug cable
 - Power Supply;
 - [MEANWELL 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.

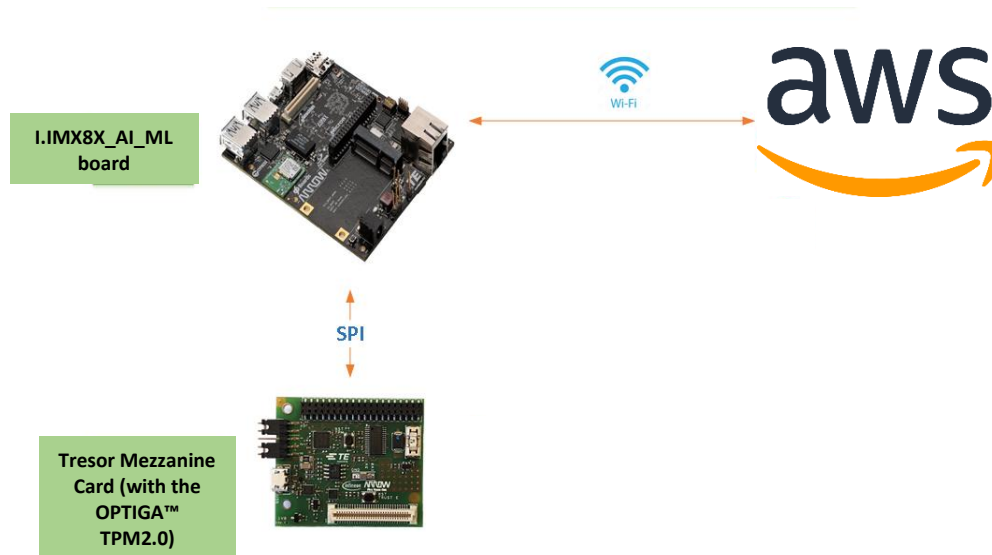


Figure 1: Setup Schematic

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. If this is not a new board out of the box, please confirm the proper hardware setup 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:

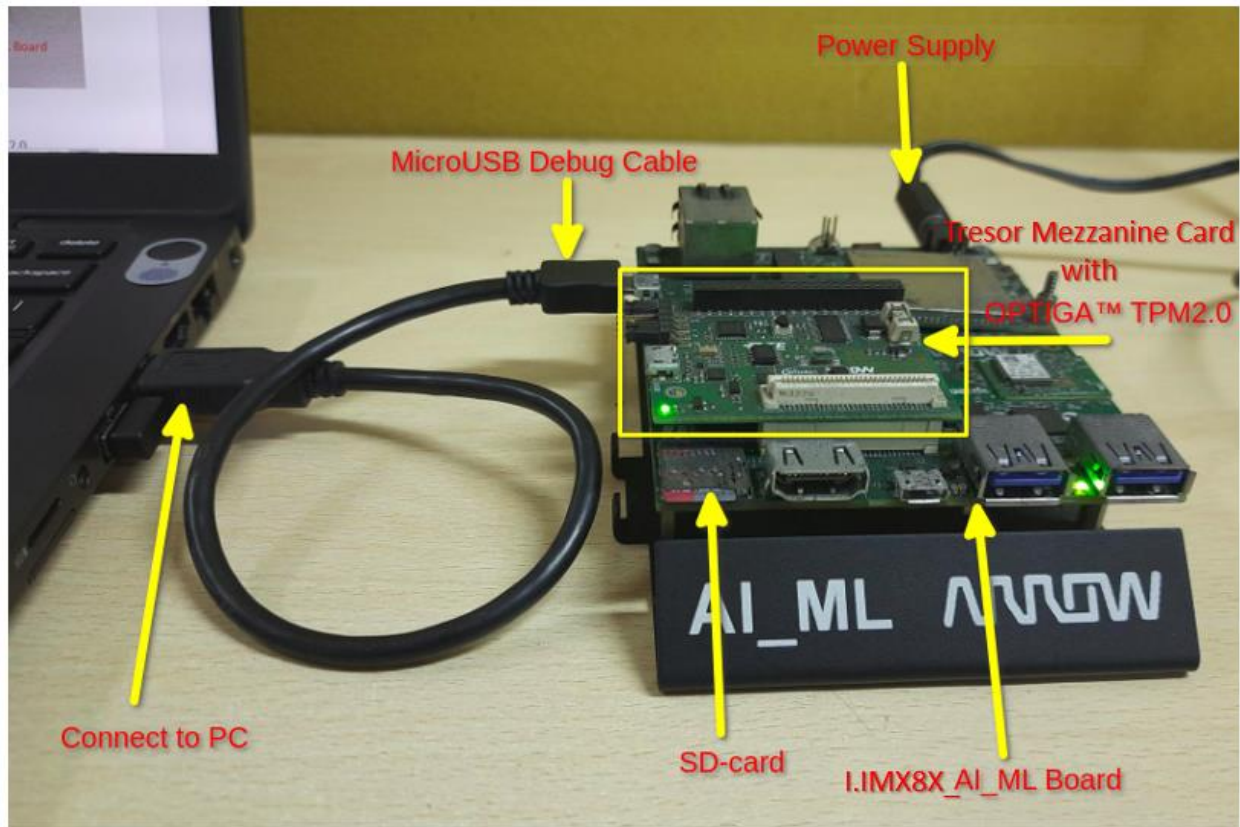


Figure 2: Hardware Setup

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 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](#) 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)

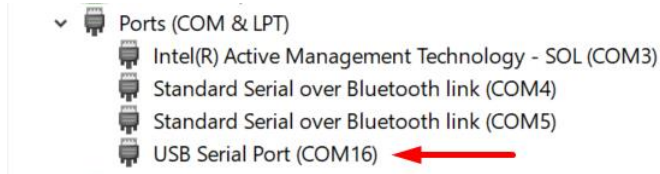
```
Linux_PC:~$ sudo minicom -s
```

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 below login console on minicom terminal on Linux PC.
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:~#
```

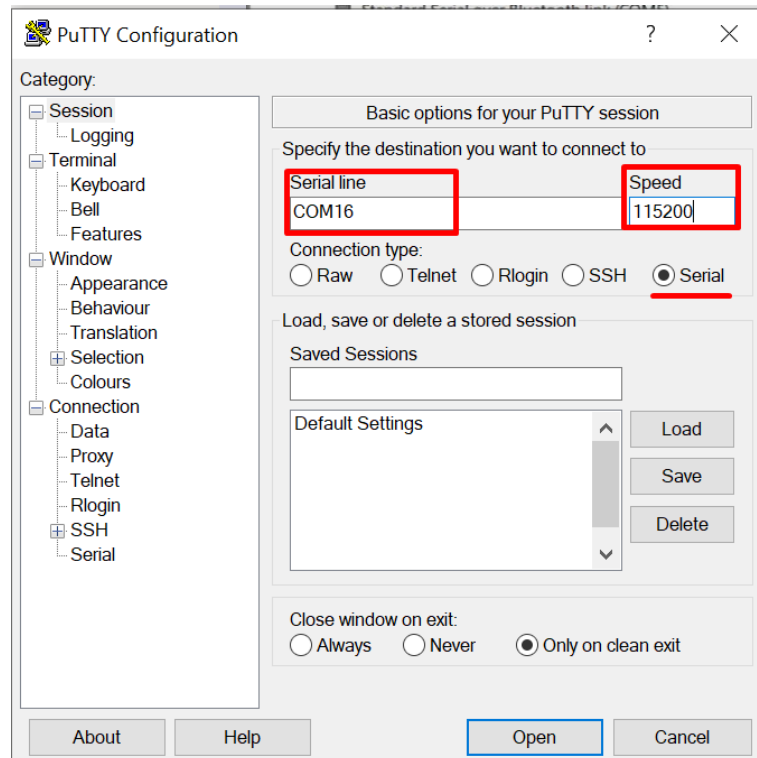
2.2.3 Software Setup on Windows Host PC (For Windows Users)

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



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.



2.2.4 Wi-Fi Setup on the AI_ML Board

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

```
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: KIPS
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 below command to ensure that the Linux PC and AI_ML board are in the same network. This is needed in 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

- File sharing between Linux Host PC and AI_ML board can be performed using Secure Shell Transfer Protocol i.e SCP 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.

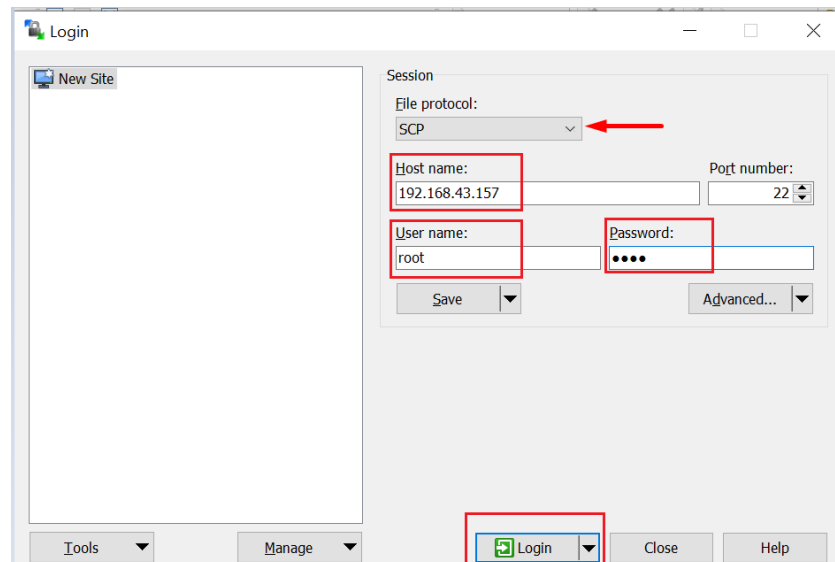
2. For Windows Host PC

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

Note:

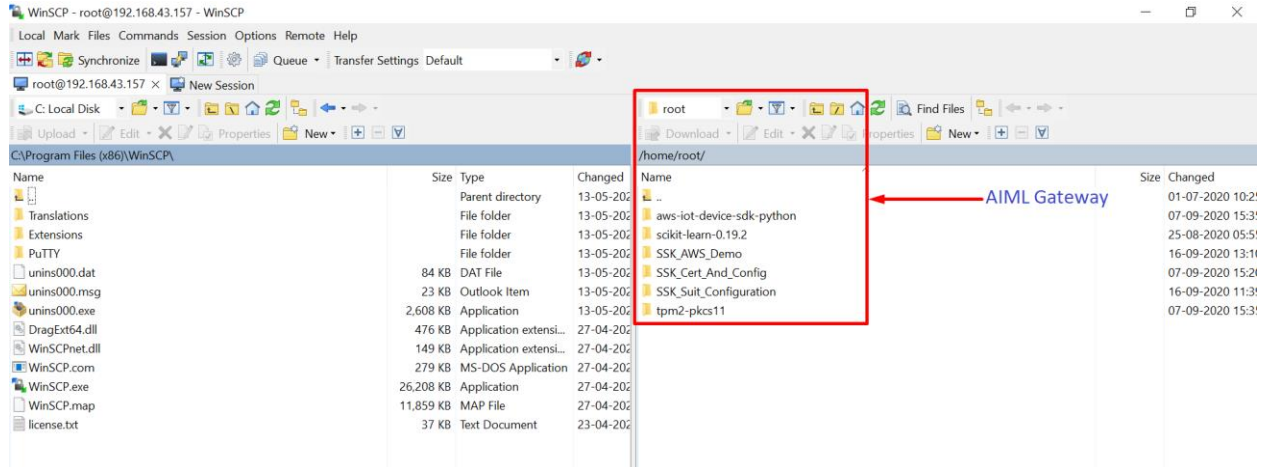
The Winscp tool can be downloaded from the link: <https://winscp.net/eng/download.php>

- Double-click on Winscp icon to start the application.
- Please enter board's IP address ("inet addr" notated in yellow above), Username (root) and Password (root-optional) and press "Login" to connect with the AI_ML Board.



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


SECURITY STARTER KIT WITH I.MX 8X AND OPTIGA™ TPM 2.0



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.

 Security Starter Kit

Home Contact

SSK

Security Starter Kit

UserName:

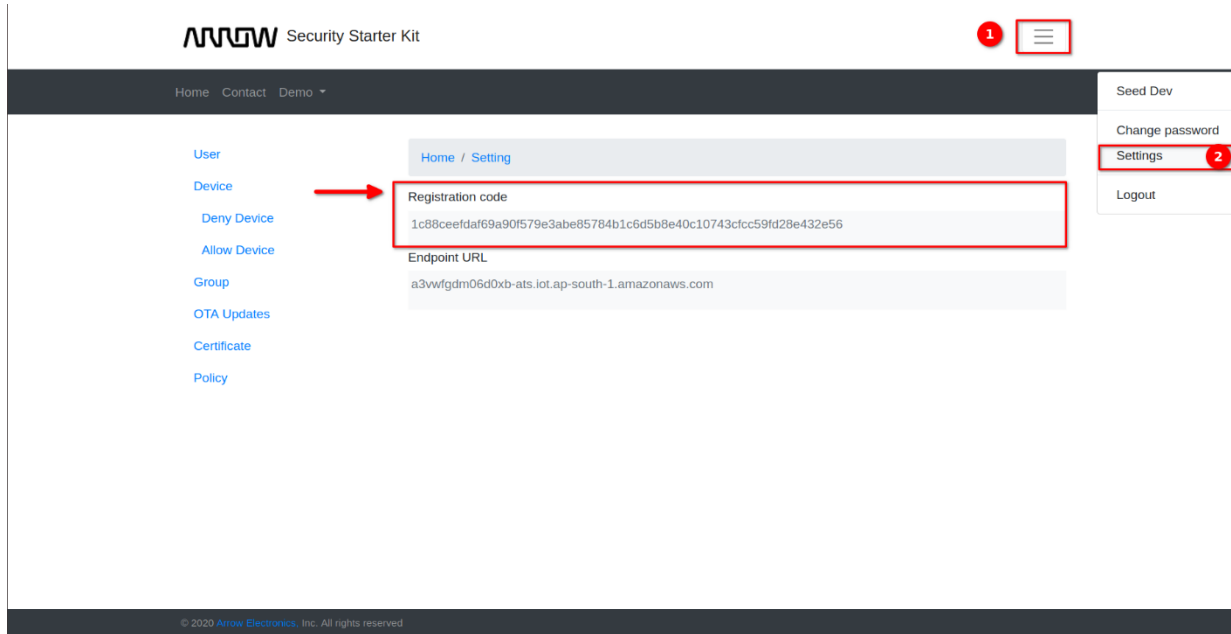
Password:

Login

© 2020 Arrow Electronics, Inc. All rights reserved

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.



- 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, please 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 Certificate Signing Request
Generate Verification Certificate signed by RootCA
Signature ok
subject=/C=IN/ST=GUJ/L=AHMEDABAD/O=Arrow/OU=eic/1c88ceefdaf69a90f579e3abe85784b1c6d5b8e40c10743cfcc59fd28e432e56
Getting CA Private Key
Copy rootCA.pem and verificationCert.crt into your HOST PC in order to uploade to Security Starter Kit Portal....
root@imx8qxpaiml:~#
```

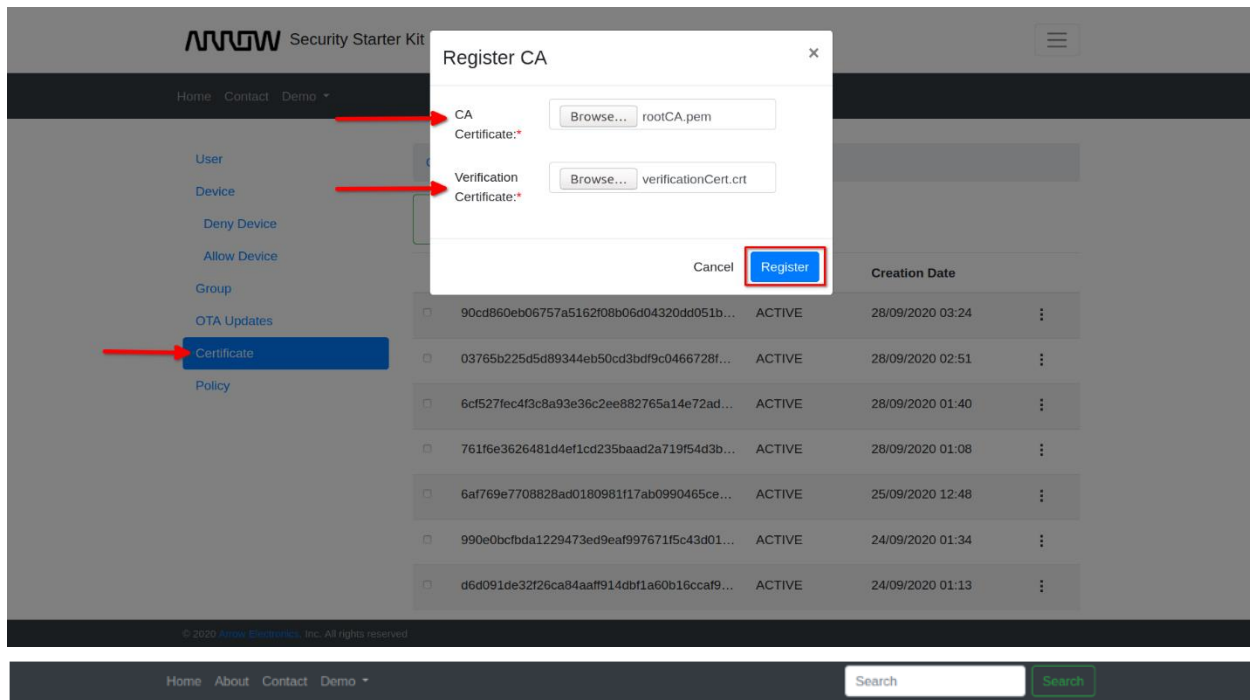
- d. Copy “/greengrass/certs/rootCA.pem” and “/greengrass/certs/verificationCert.crt” from AI_ML board to Linux PC or use winscp for Windows Host mentioned in section 2.2.4
Linux :

```
root@imx8qxpaiml:~# scp /greengrass/certs/rootCA.pem <Linux_PC_username>@<Linux_PC_IP_Addr>:/PATH
root@imx8qxpaiml:~# scp /greengrass/certs/verificationCert.crt <Linux_PC_username>@<Linux_PC_IP_Addr>:/PATH
```

Windows :

Use the “WINSOCP” tool to copy the files from AIML 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”.



CA Certificate registered successfully

[Note: Please save CA Certificate Number in the 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 Gateway device certificate using below command

```
root@imx8qxpaiml:~# 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”

The screenshot shows the ANW Security Starter Kit web interface. On the left, a sidebar menu has 'Certificate' highlighted with a red arrow. A modal dialog titled 'Register Device Certificate' is open in the center. It has a 'Device Certificate:' label and a text area containing a certificate. The certificate text is as follows:

```
-----BEGIN CERTIFICATE-----
MIIDKzCCAhMCCQD52dKgChy7+zAN
BgkqhkiG9w0BAQsFADBaMQswCQYD
VQQGEwJJ
TjEQMA4GA1UECAwHR1VKQVJBVD
EMMAoGA1UEBwwDQUhNMQ4wDAY
DVQQKDAVBUIJP
VzEMMAoGA1UECwwDRUIDMQ0wCw
YDVQQDDARTRUVEB4XD1wMDky
ODA3MDYwN1oX
-----END CERTIFICATE-----
```

At the bottom of the dialog, there are 'Cancel' and 'Register' buttons. A red arrow points to the 'Register' button. In the background, a table lists registered certificates with columns for 'Device Certificate', 'Status', and 'Creation Date'. Below the table, a green message box states 'Device Certificate registered successfully'.

[Note: Please save (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

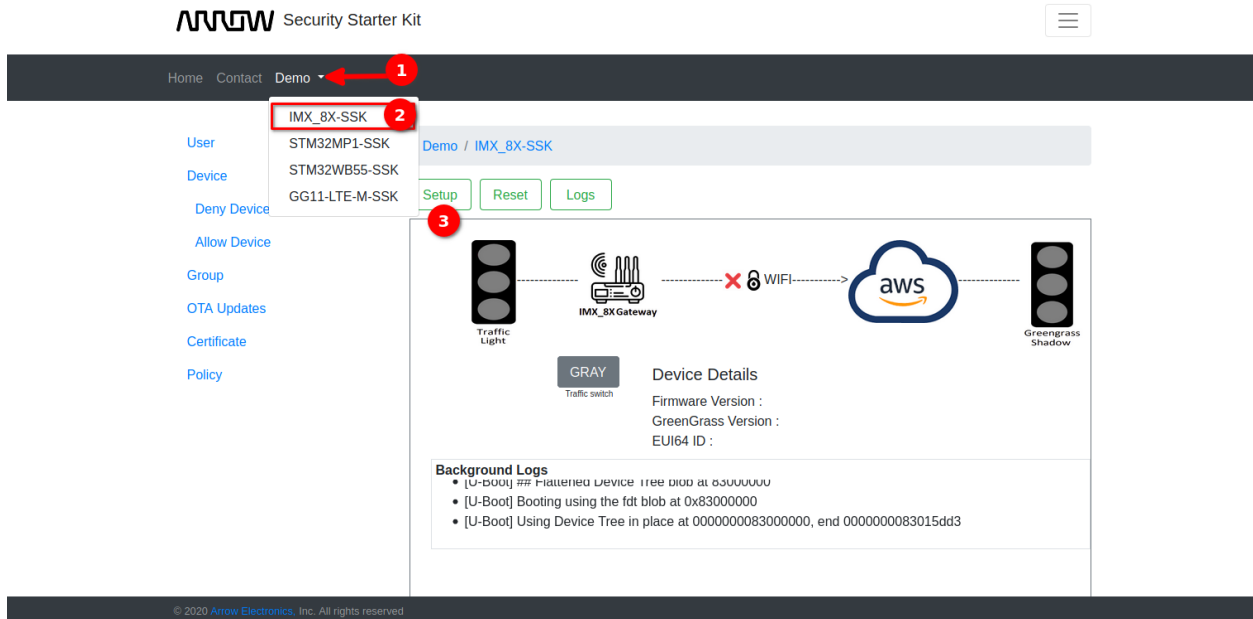
1. Collect the Gateway MAC Address using below command on AI_ML Board using minicom console on Linux PC or putty in case of Windows Host.

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

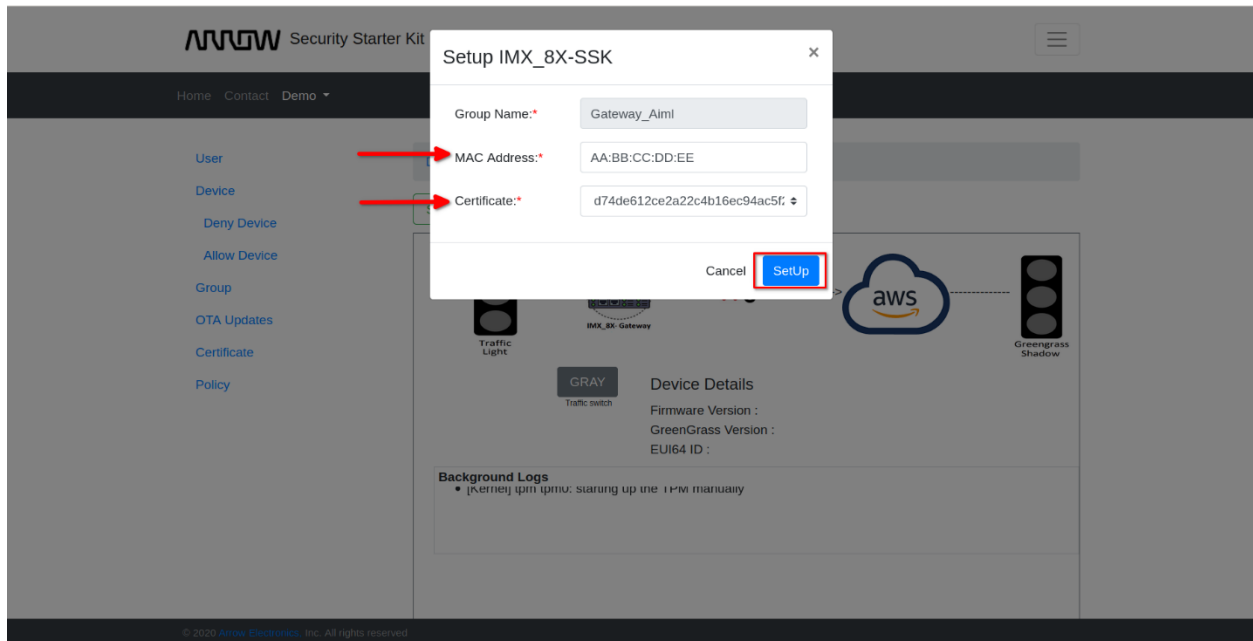
```
root@imx8qxpaiml:~# ifconfig wlan0 | grep -i HWaddr
wlan0    Link encap:Ethernet  HWaddr 00:25:ca:17:0f:ca
root@imx8qxpaiml:~#
```

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

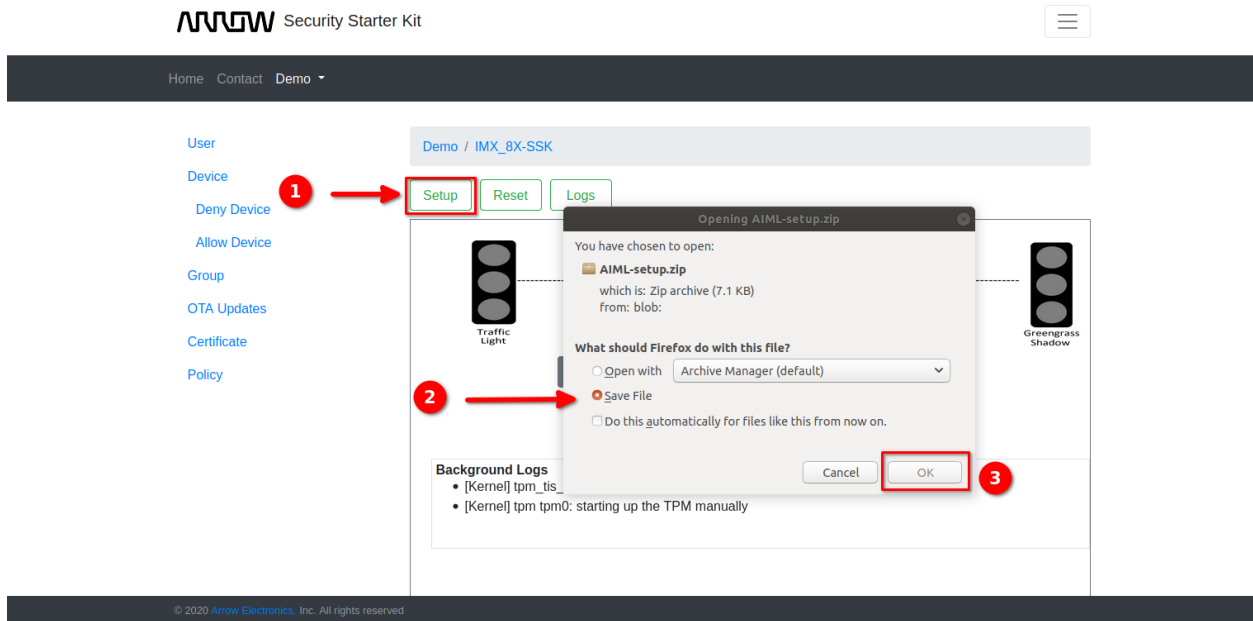
SECURITY STARTER KIT WITH I.MX 8X AND OPTIGA™ TPM 2.0



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



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



- Unzip within 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 within 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
```

Note: Difference in the silicon part number prefix mentioned above;

- 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 AIML-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 show 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=private;pin-value,
    "certificatePath" : "file:///greengrass/certs/aws_device_cert.pem"
  }
},
```

9. Zip file contains the GG_Traffic_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 SSK_AWS_Demo directory on the AI_ML board.

2.4.2 Deploying Greengrass Group

1. Run the Greengrass demo on AI_ML board using below command, before 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

User
Device
Deny Device
Allow Device
Group
OTA Updates
Certificate
Policy

Groups / List Groups

Create Group ⓘ

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	

Edit
Deployments
Subscriptions
Devices
Delete

© 2020 Arrow Electronics, Inc. All rights reserved

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

User
Device
Deny Device
Allow Device
Group
OTA Updates
Certificate
Policy

Groups / List Deployment

Back Deploy

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

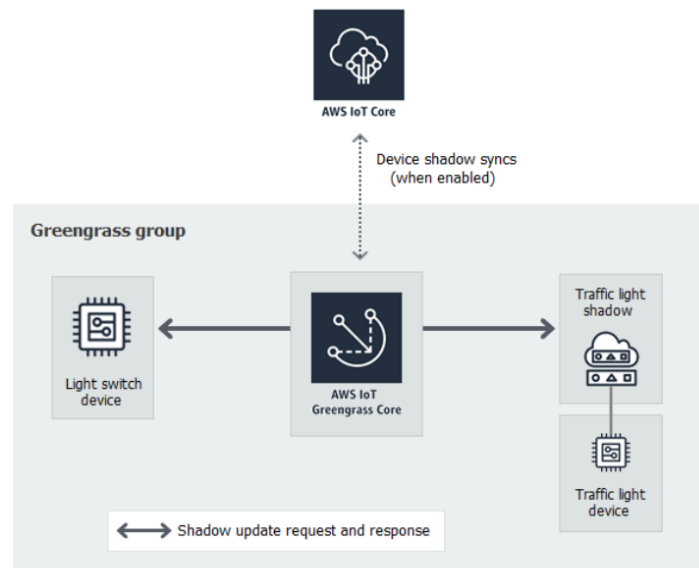
© 2020 Arrow Electronics, Inc. All rights reserved

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, shadow of the traffic light signal displayed 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, EU164 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 are continuously scrolled.

The screenshot shows the SSK Cloud Connect dashboard for the IMX_8X-SSK device. The top navigation bar includes 'Home', 'Contact', and a 'Demo' dropdown menu. The left sidebar lists various options: User, Device, Deny Device, Allow Device, Group, OTA Updates, Certificate, and Policy. The main content area displays a traffic light indicator (RED), a diagram of the IMX_8X Gateway connected to AWS via WiFi, and a 'Device Details' section. The 'Device Details' section displays: Firmware Version : Linux imx8qxpaiml 4.14.78+, GreenGrass Version : GGC version: 1.10.0-RC1, and EU164 ID : 00:25:ca:00:01:16:fd:0c. A 'Background Logs' section shows boot logs. The dashboard also includes a 'Shadow' traffic light indicator and a 'Greengrass Shadow' indicator. A yellow arrow points to the 'Demo' dropdown menu, and another yellow arrow points to the 'Device Details' section.

- 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-4305-85f1-7f125748b2c6'}}
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...
-----
```

SECURITY STARTER KIT WITH I.MX 8X AND OPTIGA™ TPM 2.0

- If a user wants to reset the Setup
Please follow [SSK Cloud Connect >> Demo >> IMX_8X-SSK >> Press “Reset” button](#)
- Kill the demo process (or by pressing “CTRL + C”) and reboot the AI_ML board, using below command.

```
root@imx8qxpaiml:~# reboot -f
```

The screenshot displays the Arrow Security Starter Kit web interface. At the top, the Arrow logo and "Security Starter Kit" are visible. A navigation bar includes "Home", "Contact", and "Demo". A green notification banner at the top states "Gateway_Aiml Setup reset completed successfully". The main content area is titled "Demo / IMX_8X-SSK" and features three buttons: "Setup", "Reset" (highlighted with a red box), and "Logs". Below these buttons is a diagram showing the system architecture: a "Traffic Light" icon connected to an "IMX_8X Gateway" icon, which is connected to an "aws" cloud icon, and finally to a "Greengrass Shadow" icon. A "Traffic switch" icon labeled "GRAY" is also present. To the right of the diagram, "Device Details" are listed: "Firmware Version :", "GreenGrass Version :", and "EUI64 ID :". Below the diagram, "Background Logs" are shown, including boot logs for SCFW, SECO-FW, IMX-MKIMAGE, ATF, and U-Boot.

© 2020 Arrow Electronics, Inc. All rights reserved

2.4.5 Demo Inference

Security Starter 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 store the session credentials, secure communication between AWS and the AI_ML board is achieved. .
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>

- [Developer Guide iMX8X SSK.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](#)