

---

# TrustFLEX Step by Step Guide

## Azure IoT with Custom PKI

---

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
1.1	Getting started with Jupyter Notebook Tutorials .....	3
1.1.1	Starting Jupyter Notebook.....	3
1.2	Jupyter Notebook Basics .....	3
1.2.1	The Notebook dashboard .....	3
1.3	Introduction to Jupyter Notebook GUI .....	4
<b>2</b>	<b>Jupyter Notebook Tutorials .....</b>	<b>6</b>
<b>3</b>	<b>Resource Generation Notebook .....</b>	<b>7</b>
<b>4</b>	<b>Use Case Prototyping .....</b>	<b>14</b>
4.1	Running Custom PKI example on Jupyter Notebook .....	14
4.2	Running Custom PKI example on Embedded platform .....	19
4.2.1	Atmel Studio: .....	20
4.2.2	MPLAB: .....	23
4.3	CryptoAuth Trust Platform Factory reset .....	25
<b>5</b>	<b>FAQ.....</b>	<b>27</b>

---

# 1 Introduction

This document gives a detailed walk through of the custom public key infrastructure use case implementation. If familiar with Jupyter Notebook, can skip this section and move to Section 2.

## 1.1 Getting started with Jupyter Notebook Tutorials

Jupyter Notebook is open source web application which allows you to create documents that contain code that you can execute in place as well as narrative text. It provides GUI elements, ability to execute code in place, ability to add images and gives it the look and feel that normal code files lack.

Jupyter notebooks are mainly used to explain/evaluate code in an interactive way.

### 1.1.1 Starting Jupyter Notebook

Jupyter notebook can be launched from the Anaconda Navigator main window.



## 1.2 Jupyter Notebook Basics

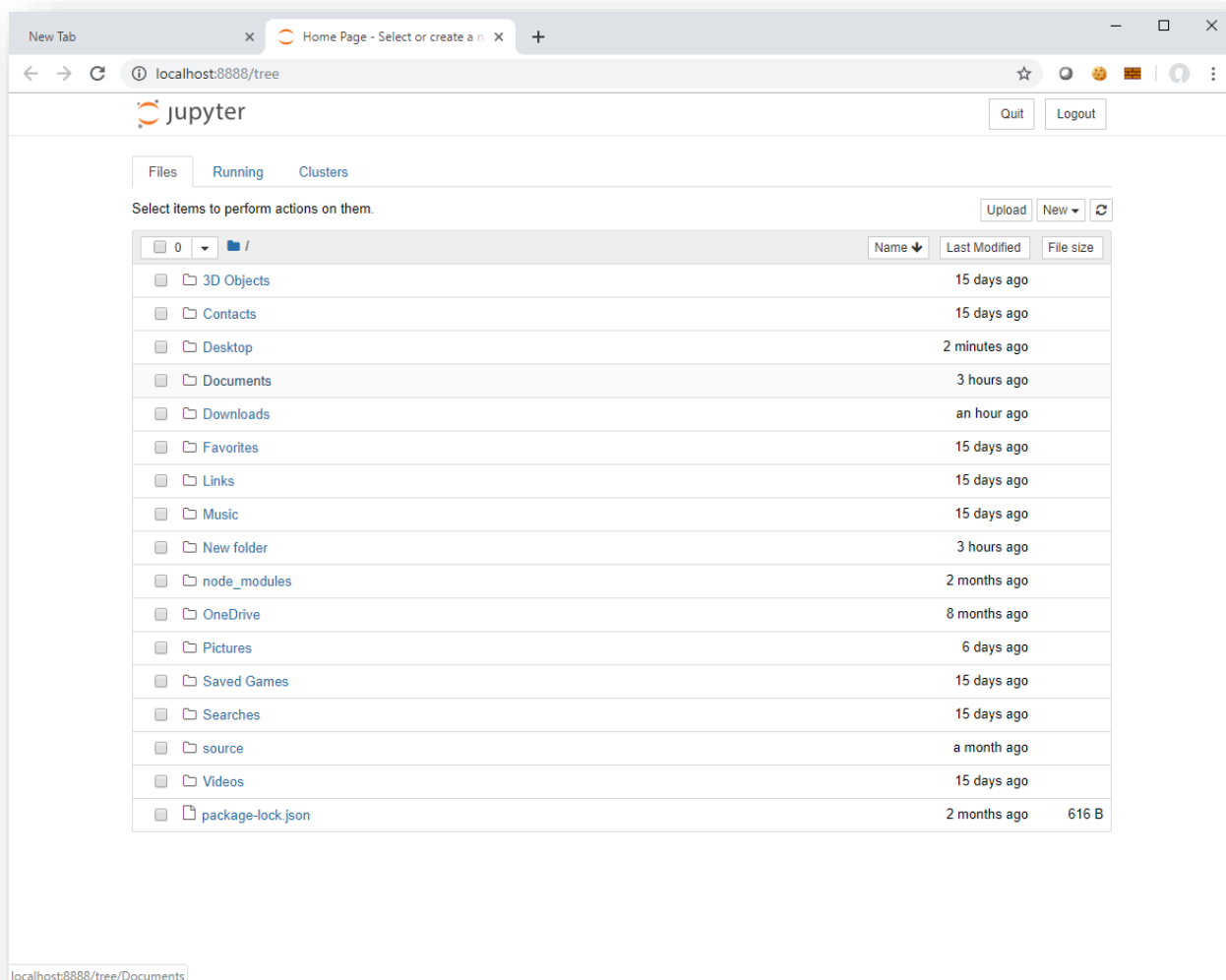
It is recommended to become familiar with Jupyter basic concepts with the online documentation, <https://jupyter-notebook.readthedocs.io/en/stable/examples/Notebook/Notebook%20Basics.html>

Some of the content is duplicated here for convenience. The online documentation should always be used as a reference.

### 1.2.1 The Notebook dashboard

When you first start the notebook server, your browser will open Notebook dashboard. The dashboard serves as a home page for the notebook. Its main purpose is to display the notebooks and files in the current directory.

For example, here is a screenshot of the Jupyter dashboard. The top of the notebook list displays clickable breadcrumbs of the current directory. By clicking on these breadcrumbs or sub-directories in the notebook list, you can navigate your file system.

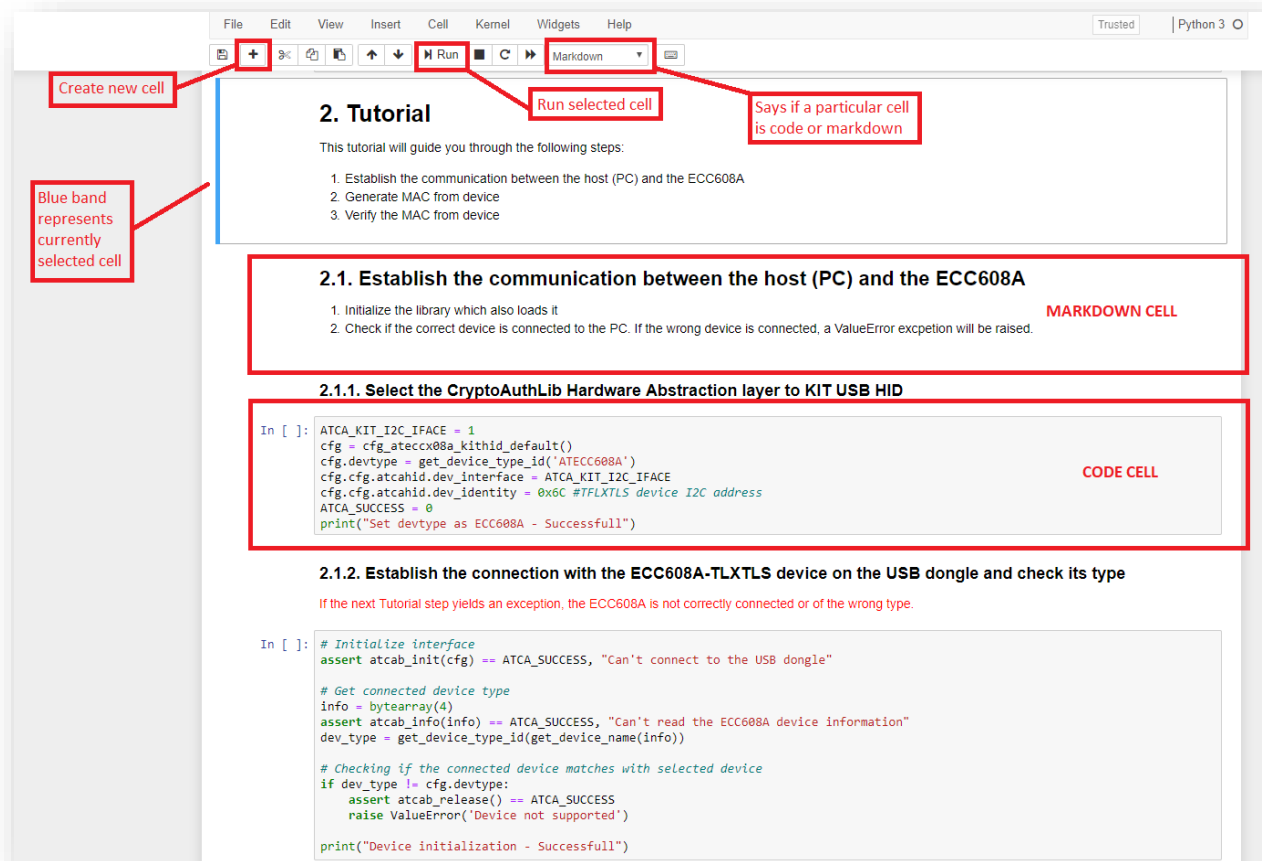


### 1.3 Introduction to Jupyter Notebook GUI.

Jupyter Notebooks contain cells where you can either write code or markdown text. Notebooks contain multiple cells, some set as code and others markdown. Code cells contain code that can be executed live, and markdown contains text and images that explains the code.

Below image shows some options in a typical Jupyter Notebook. Individual cells can be executed by pressing on the RUN button as shown in the below image.

All cells in the Notebook can be executed in order by **Kernel->Restart & Run All**.



To run all cells in sequence.



## 2 Jupyter Notebook Tutorials

The TrustPlatform Design Suite comes with a number of Notebook Tutorials to easily prototype popular use cases for TrustFLEX and Trust&Go devices. Here is the list of Jupyter Notebook Tutorials.

<b>Jupyter Notebook Tutorials</b>	<b>Relative Path</b>	<b>Applicable Devices</b>
Manifest Generation	TrustnGO\00_resource_generation\TNGTLS_manifest_file_generation.ipynb	TrustnGO
Resource Generation	TrustFLEX\00_resource_generation\TFLXTLS_resource_generator.ipynb	TrustFLEX
Accessory Authentication	TrustFLEX\01_accessory_authentication\notebook\TFLXTLS_accessory_authentication.ipynb	TrustFLEX
Firmware Validation	TrustFLEX\02_firmware_validation\notebook\TFLXTLS_firmware_validation.ipynb	TrustFLEX
GCP Connect	TrustFLEX\03_gcp_connect\notebook\TFLXTLS_GCP_connect.ipynb	TrustFLEX
IP Protection	TrustFLEX\04_ip_protection\notebook\TFLXTLS_IP_protection.ipynb	TrustFLEX
Secure Public Key Rotation	TrustFLEX\05_public_key_rotation\notebook\TFLXTLS_public_key_rotation.ipynb	TrustFLEX
AWS Custom PKI	TrustFLEX\06_custom_pki_aws\notebook\TFLXTLS_aws_connect.ipynb	TrustFLEX
Azure Connect	TrustFLEX\07_custom_pki_azure\notebook\TFLXTLS_azure_connect.ipynb	TrustFLEX

---

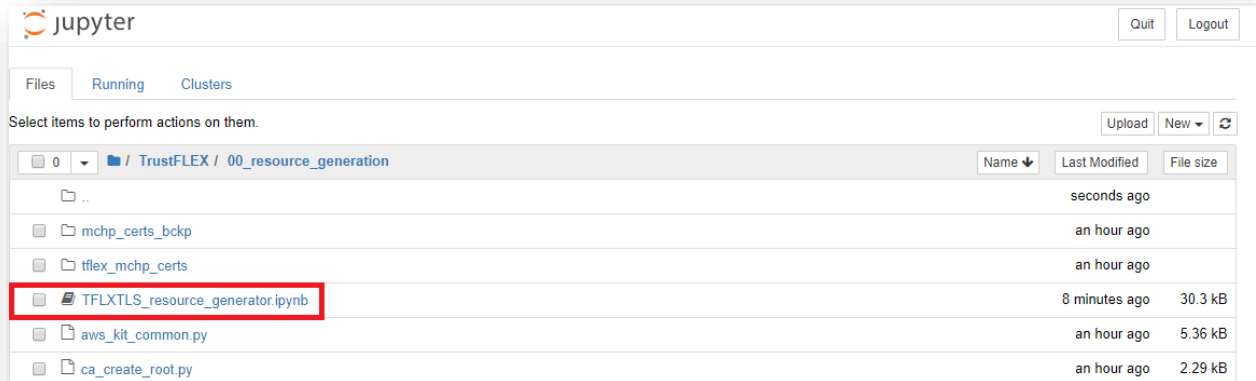
### 3 Resource Generation Notebook

TFLXTLS device is one of the three devices available in the Trust Platform USB Dongle Board.

TrustFLEX devices come pre-programmed with certificates in slots 10, 11 and 12, also slots 0-4 have pre-generated private keys, other than the mentioned slots all the other slots have no meaningful data in them.

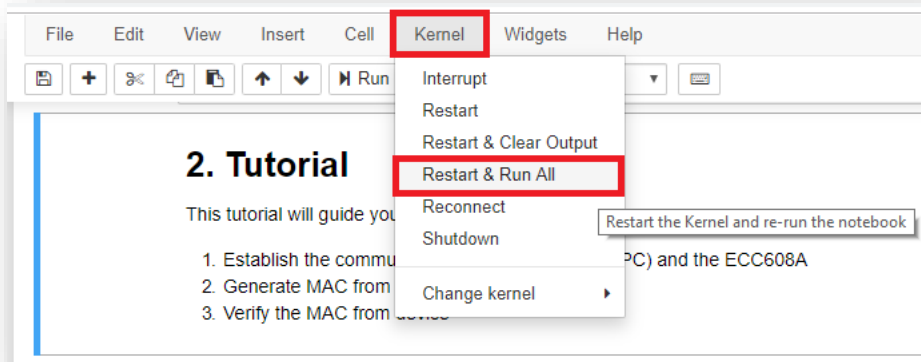
The Resource Generator Notebook will create development keys and certificates for all slots that can be further customized. Keys and Certificate chains are stored in the PC filesystem. These keys should never be used for production purposes as their generation is not handled in a secure environment. These development keys will be later used by the other notebooks to implement the various pre-defined use cases.

Within the Jupyter Dashboard, navigate **TrustFLEX\00\_resource\_generation** folder to open **TFLXTLS\_resource\_generator.ipynb** notebook

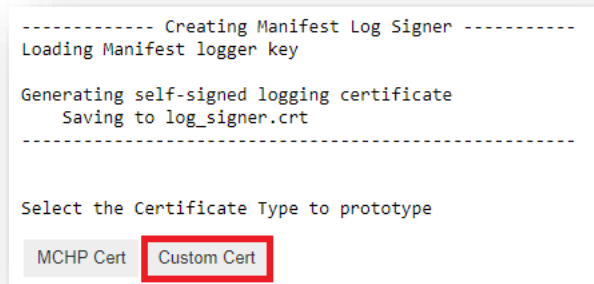


Run all cells of the Crypto Resource Generator Notebook: Kernel->Restart & Run All

**Note:** Before executing the cells on Crypto Trust Platform, its required to have factory default program running on SAMD21 of Trust Platform. Refer to [4.3 CryptoAuth TrustPlatform Factory reset](#) section for reloading default program.



It will execute and prompt you to choose between MCHP certificate and a custom certificate chain, press "Custom Cert" option for this use case.



Now it prompts you to enter the organization name, enter the name that will be used as an Organization Name in the certificate template. The name length is limited to 24 characters.

The Notebook will generate several keys and certificates. Make sure you have an error free output before continuing to the next steps of the training.

The output log should resemble this:

-----  
-----

Loading root CA key

Generating self-signed root CA certificate



---

Saving to root-ca.crt

Loading signer CA key

Generating signer CA CSR

Saving to signer-ca.csr

Loading signer CA CSR

Loading from signer-ca.csr

Loading root CA key

Loading from root-ca.pem

Loading root CA certificate

Loading from root-ca.crt

Generating signer CA certificate from CSR

Saving to signer-ca.crt

-----

Signer Certificate written successfully to device

Device Certificate written successfully to device

Thing ID c162f7cedb44317696f7fcf7c80c43cbee4a6c97

-----

Generating signer certificate definition header file - cust\_def\_1\_signer.h

Generating device certificate definition header file - cust\_def\_2\_device.h

Generating signer certificate definition source file - cust\_def\_1\_signer.c

Generating device certificate definition source file - cust\_def\_2\_device.c

-----

Custom certificate generation and provisioning - SUCCESS

-----

Root Certificate loading from: root-ca.crt

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

46:ae:32:e9:71:02:da:03:24:27:f0:1c:0b:b9:84:9d



---

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

67:f4:54:1e:c6:7b:9c:53:1a:eb:6c:71:c6:53:7e:11

Signature Algorithm: ecdsa-with-SHA256

Issuer: O = "custom\_org", CN = Crypto Authentication Root CA 000

Validity

Not Before: Nov 19 06:00:00 2019 GMT

Not After : Nov 19 06:00:00 2029 GMT

Subject: O = "custom\_org", CN = Crypto Authentication Signer FFFF

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:79:5c:1d:e1:c4:42:9c:fd:a4:25:26:92:a8:1c:  
a5:bb:a5:e2:f4:00:24:b9:a9:93:45:44:45:94:d1:  
61:5f:89:73:92:9d:f5:7d:90:6c:c0:be:93:89:ef:  
69:cc:ce:80:b7:03:c6:2e:9e:b1:01:de:be:b0:4d:  
20:26:33:b4:f9

ASN1 OID: prime256v1

NIST CURVE: P-256

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

X509v3 Basic Constraints: critical

CA:TRUE, pathlen:0

X509v3 Subject Key Identifier:

1C:27:0D:E4:22:01:30:6A:37:0F:F9:68:E4:D8:91:04:C9:37:D5:82

X509v3 Authority Key Identifier:

keyid:8F:28:E9:74:55:D1:49:52:9D:09:3C:70:00:9F:BB:11:79:9B:FB:3B

Signature Algorithm: ecdsa-with-SHA256

30:45:02:21:00:c6:8d:c9:fd:a0:07:6f:6d:ab:c3:4e:cd:bf:  
d1:eb:61:a1:80:1b:fd:b0:6f:b3:6e:eb:fe:2c:ef:4b:f7:2d:  
6f:02:20:66:ed:8f:4a:60:1a:34:56:e3:6d:2b:e9:01:ba:3b:  
5b:37:b2:b7:7b:bf:a5:58:d7:37:cd:55:9b:a8:e4:15:eb

-----BEGIN CERTIFICATE-----

MIICAjCCAaigAwIBAgIQZ/RUHsZ7nFMa62xxxIN+ETAKBggqhkJOPQQDAjBPMSEw  
HwYDVQQKBHjdXN0b21fb3JnICAgICAgICAgICAgICAxKjAoBgNVBAMMIUNyeXB0  
byBBdXR0ZW50aWNhdGlvb1BSb290IENBIDAeMDAeFw0xOTExMTkwNjAwMDBaFw0y  
OTExMTkwNjAwMDBaME8xITAfBgNVBAoMGGN1c3RvbV9vcmcgICAgICAgICAgICAg  
IDEqMCgGA1UEAwwhQ3J5cHRvIEF1dGh1bnRyY2F0aW9uIFNpZ25lciBGRkZGMFkw  
EwYHKOZIZj0CAQYIKoZIZj0DAQcDQgAEeVwd4cRCnP2kJSaSqBylu6Xi9AAkuamT

RURFINFhX4lzkp31fZBswL6Tie9pzM6AtwPGLp6xAd6+sE0gJj00+aNmMGQwDgYD  
VR0PAQH/BAQDAgGGMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFBwnDeQi  
ATBqNw/5aOTYkQTJN9WCMB8GA1UdIwQYMBaAFI8o6XRV0UISnQk8cACfuxF5m/s7  
MAoGCCqGSM49BAMCA0gAMEUCIQDGjcn9oAdvbavDTs2/0ethoYAb/bBvs27r/izv  
S/ctbwIgZu2PSmAaNfbjbSvpAbo7Wzeyt3u/pVjXN81Vm6jkFes=  
-----END CERTIFICATE-----

Validate Signer Certificate:  
OK

Device Certificate loading from: device\_cert.crt  
Certificate:

Data:

Version: 3 (0x2)

Serial Number:

4b:58:a6:d8:9c:be:92:41:bc:f8:57:54:df:02:2b:3e

Signature Algorithm: ecdsa-with-SHA256

Issuer: O = "custom\_org", CN = Crypto Authentication Signer FFFF

Validity

Not Before: Nov 19 06:00:00 2019 GMT

Not After : Nov 19 06:00:00 2029 GMT

Subject: O = "custom\_org", CN = 01239E0A9490433401\_ATECC

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:0f:eb:6a:61:45:3e:f7:97:58:f9:dc:98:13:98:  
e0:20:10:99:7a:49:3e:c8:ab:29:01:79:bc:4e:13:  
7a:1e:cf:c3:e3:2e:89:66:7b:6e:cf:9c:0f:c3:10:  
15:c0:35:64:ac:28:b8:9f:8e:f4:68:d5:f3:d9:a2:  
4f:17:28:a9:0d

ASN1 OID: prime256v1

NIST CURVE: P-256

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:

C1:62:F7:CE:DB:44:31:76:96:F7:FC:F7:C8:0C:43:CB:EE:4A:6C:97

X509v3 Authority Key Identifier:

keyid:1C:27:0D:E4:22:01:30:6A:37:0F:F9:68:E4:D8:91:04:C9:37:D5:82

Signature Algorithm: ecdsa-with-SHA256

---

```
30:45:02:20:3f:e6:c7:a5:17:80:57:d6:69:04:36:01:34:5e:
0e:c2:f3:8a:17:2f:a5:6b:41:ca:9e:79:23:42:1d:60:1e:6e:
02:21:00:bb:d6:59:98:a0:a1:34:4e:81:b8:c9:1d:ae:54:18:
7f:f2:57:46:34:5e:e9:03:ff:7f:39:4e:eb:d2:a3:72:8d
```

-----BEGIN CERTIFICATE-----

```
MIIB8zCCAZmgAwIBAgIQS1im2Jy+kkG8+FdU3wIrPjAKBggqhkJOPQQDAjBPMSEw
HwYDVQQKBHjdXN0b21fb3JnICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
byBBdXR0ZW50aWNhdGlvb21fb3JnICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
OTExMTkwNjAwMDEyMTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5
IDEhMB8GA1UEAwYyMDEyMTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5MTA5
AQYIKoZIzj0DAQcDQgAED+tgYUU+95dY+dyYE5jgIBCZekk+yKspAXm8ThN6Hs/D
4y6JZntuz5wPwxAVwDVkrCi4n470aNXz2aJPFyipDaNgMF4wDAYDVR0TAQH/BAIw
ADAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0OBBYEFMF987bRDF2lvf898gMQ8vuSmyX
MB8GA1UdIwQYMBaAFBwnDeQiATBqNw/5aOTYkQTJN9WCMAoGCCqGSM49BAMCA0gA
MEUCID/mx6UXgFfWaqQ2ATReDsLzihcvpWtByp55I0IdYB5uAiEAu9ZZmKChNE6B
uMkdrIQYf/JXRjRe6QP/fzIO69Kjco0=
```

-----END CERTIFICATE-----

Validate Device Certificate:

OK

Generated the manifest file 01239e0a9490433401\_manifest.json

Custom Certificate processing completed successfully

-----

At the end of the execution, a Custom PKI chain will be generated on your PC and TrustFLEX device specific slots (10 through 12) will be overwritten with the custom certificates.

The Notebook has also generated a manifest file to be uploaded into the public cloud of your choice (Google GCP, AWS IoT and Microsoft Azure).

## 4 Use Case Prototyping

This hands-on lab is intended to demonstrate the usage of TrustFLEX to secure an Azure IoT connection based on a custom PKI.

The Azure IoT device reference implementation is provided as an MPLAB X project and the generation of a custom PKI is achieved through the execution of Jupyter Notebook Tutorials.

Here are the steps that will be required to complete this Tutorial:

- Configure Azure CLI
- Register Custom PKI signer
- Build the Azure IoT device source code and flash it to the USB Dongle Board

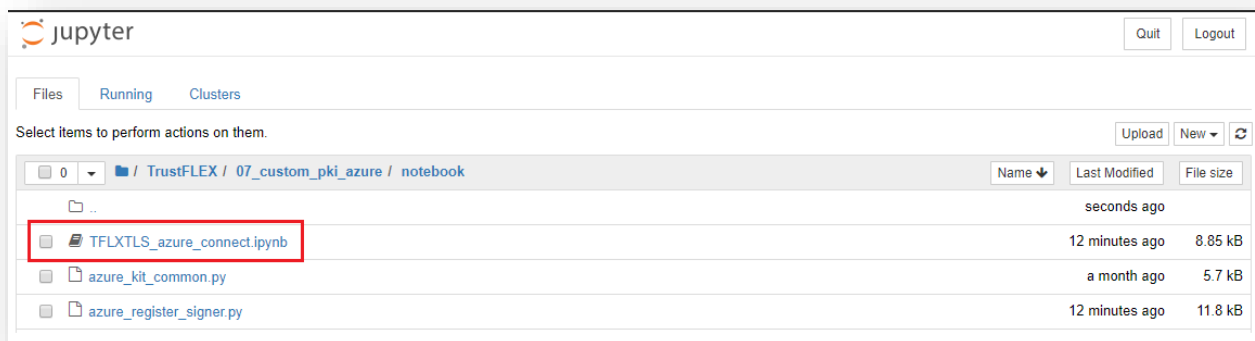
Note: It is required to have an Azure IoT test account setup. Instruction to setup the account quickly is provided in

**docs\TrustFLEX\_guide\_Azure\_demo\_account\_setup.pdf**. Once the account is setup, IoT hub HostName should be updated in **docs\Azure\_iot\_hub\_details.csv**

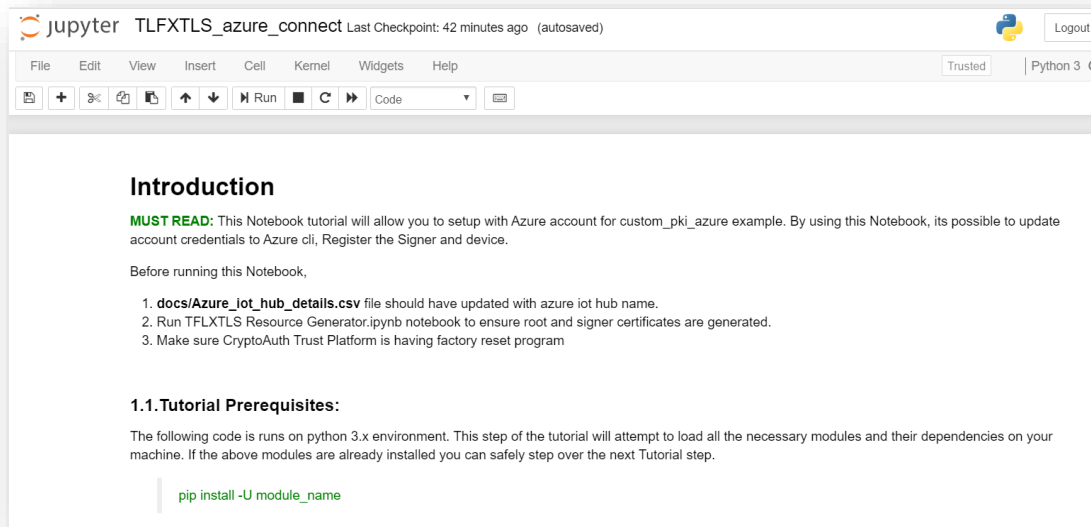
### 4.1 Running Custom PKI example on Jupyter Notebook

By running this following step, we can configure the Azure command line with Azure credentials, register the signer certificate to Azure IoT.

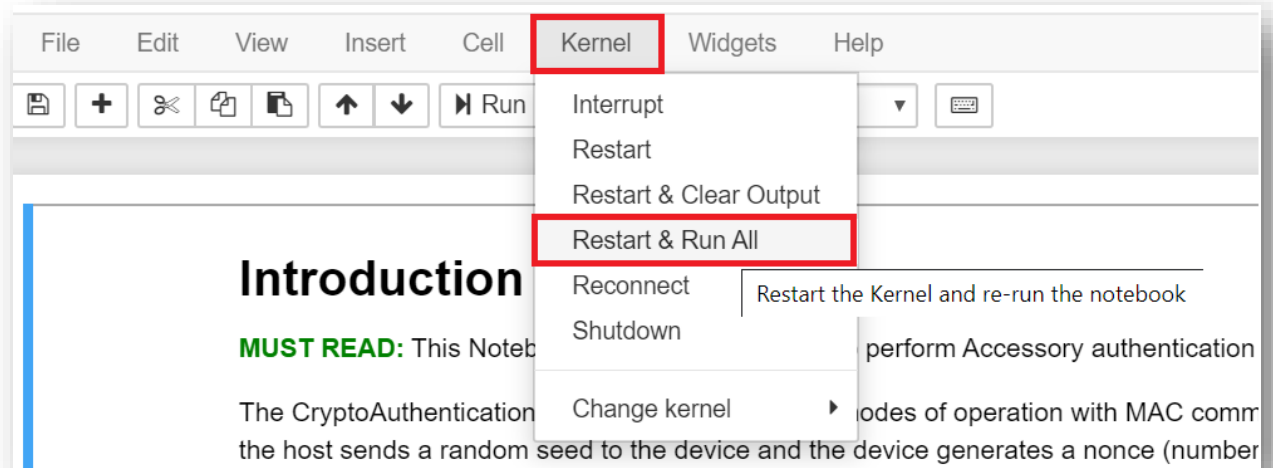
1. From the Jupyter Home page, navigate to **TrustFLEX\07\_custom\_pki\_azure\notebook\TFLXTLS\_azure\_connect.ipynb** notebook file and open it.



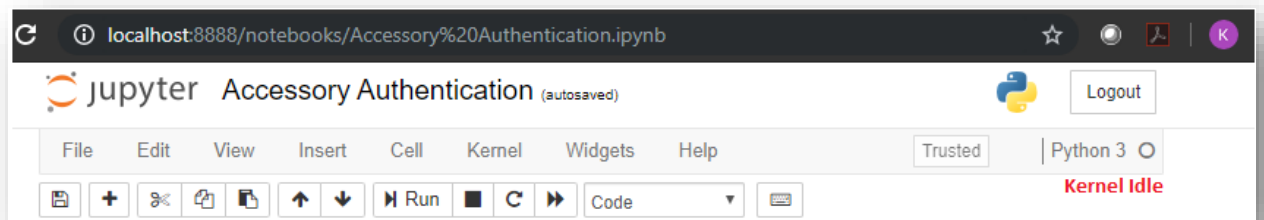
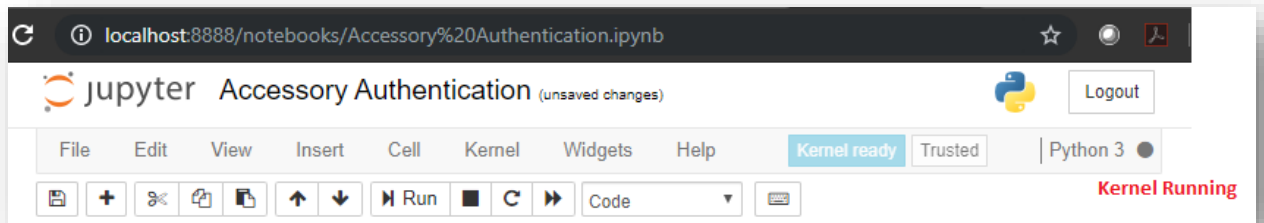
Opening the Jupyter notebook example should load the following on the browser.



## 2. Run All Cells by using Kernel -> Restart & Run All



It may take a while to complete, wait for the kernel to complete all processing i.e. from Kernel Running to Kernel Idle state (Check circle above **RED** text)

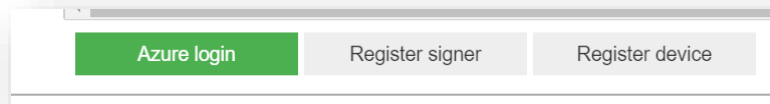


3. Navigate through different cells output for the description of the step and result from the execution.

4. There are 3 major steps:

Configure Azure command line interface:

Before we can interact with Azure, we need to configure the tools with the appropriate Azure credentials. These credentials are composed of the **azure account login**. Clicking the button will open azure login portal in new tab in browser. Enter the credentials of your account.

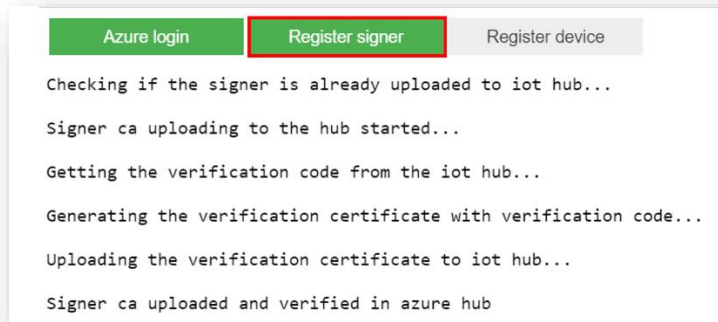


Register Signer Module:

Code block of this step generates "**Register signer**" button. Clicking the button, it registers the custom PKI signer module to the Azure account. To establish a secure communication with Azure IoT, we need to register the Custom PKI signer certificate to Azure IoT

Upon successful execution, the log should look like this.





Once this step is completed, signer module is successfully registered to Azure IoT.

### Register Device:

Code block of this step generates "**Register Device**" button. Clicking the button Registers the device to the azure iot hub and output log should be as below.

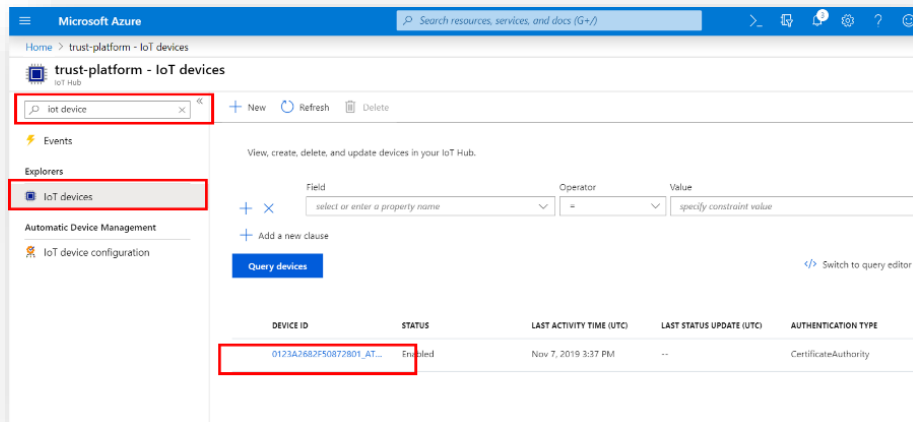


**NOTE:** Make sure that you executed C project successfully before executing the next step .To execute C project, refer "[Running Azure IoT example on Embedded platform](#)" section.

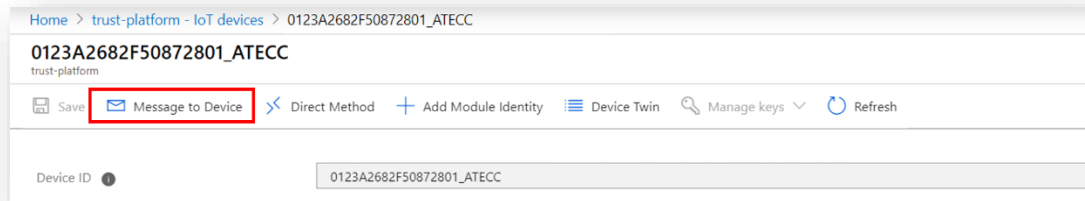
### Control Trust Platform Azure Cloud

In this section we are going to control the status led on the Trust platform device from the Azure cloud.

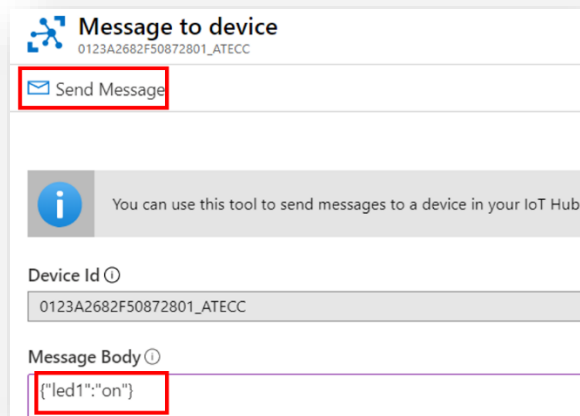
1. In the <https://portal.azure.com/> select your IoT hub created, search for iot device and select **IoT devices** from Explorers.
2. From the Device ID select the device id that want to be controlled. The Device ID Should be same as the highlighted one previous step **Register Device**



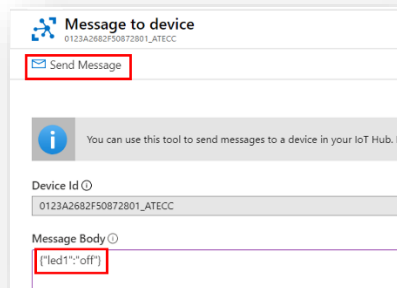
3. In the Device ID window, select the Message to Device



4. Now to Turn the led on the Trust platform board. Paste the message `{"led1":"on"}` to the message body and click Send Message.



5. Now to Turn the led on the Trust platform board. Paste the message `{"led1\":\"off\"}` to the message body and click Send Message



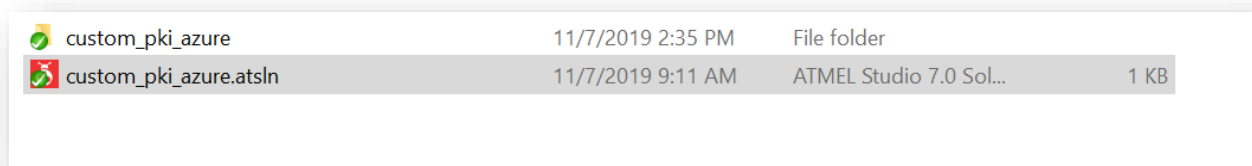
## 4.2 Running Custom PKI example on Embedded platform

Once the resources are generated both Atmel Studio and MPLAB projects provided can be used to run the use case on CryptoAuth Trust Platform.

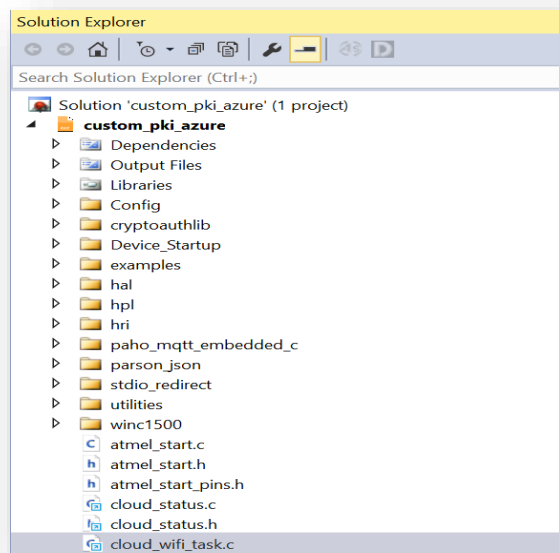
This project can configure the Wi-Fi credentials, establish a TLS connection, subscribe to MQTT. It is required to use the Azure IoT Jupyter notebook to register the signer module.

#### 4.2.1 Atmel Studio:

1. Open **custom\_pki\_azure.atsln** project by navigating  
**TrustFLEX\07\_custom\_pki\_azure\c\studio\custom\_pki\_azure.atsln**



2. In the project navigate to **custom\_pki\_azure -> cloud\_wifi\_task.c** file



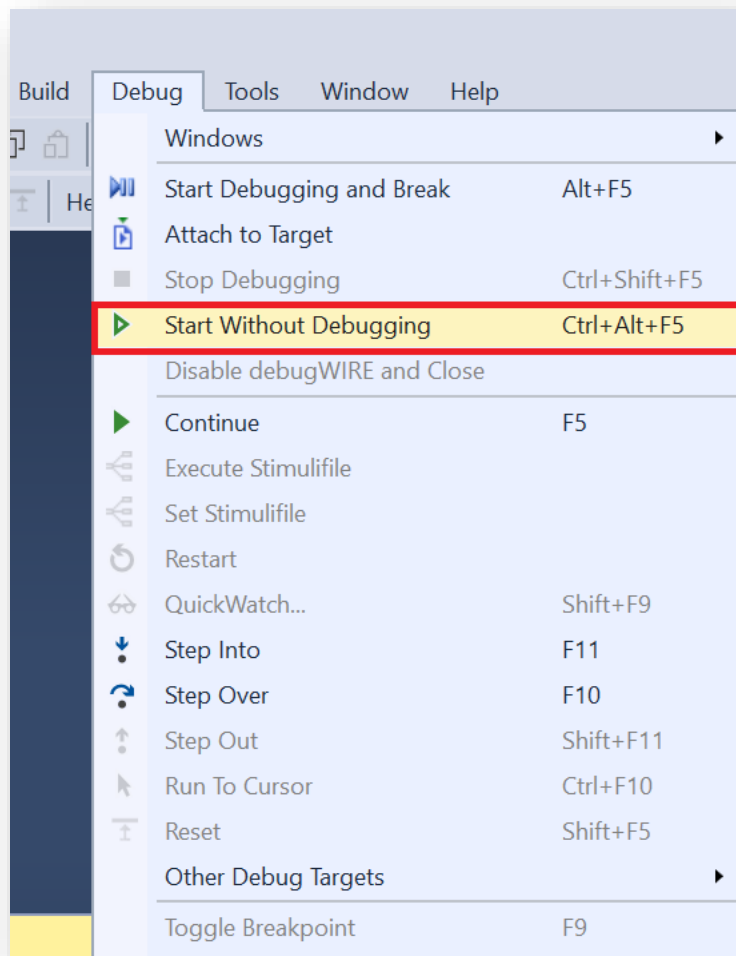
update the following constants before building the project:

- MAIN\_WLAN\_SSID
- MAIN\_WLAN\_PSK
- CLOUD\_ENDPOINT

The Highlighted area in CLOUD\_ENDPOINT string should have the Azure IOT Hub Name. The IoT Hub name can be got from the azure portal or from the docs/Azure\_iot\_hub\_details.csv file.

```
#define CLOUD_ENDPOINT "xxxxxxxxxxxx.azure-devices.net"
```

3. Program the CryptoAuth Trust Platform by navigating to **Debug -> Start Without Debugging**



This step may take some time, wait for Atmel Studio to compile and program the device.

Once the programming is done, reset the hardware (press the reset button) and view the Console messages by using applications like 'Tera Term'. Open the application with the COM related to CryptoAuth Trust Platform with 115200-8-N-1 settings.

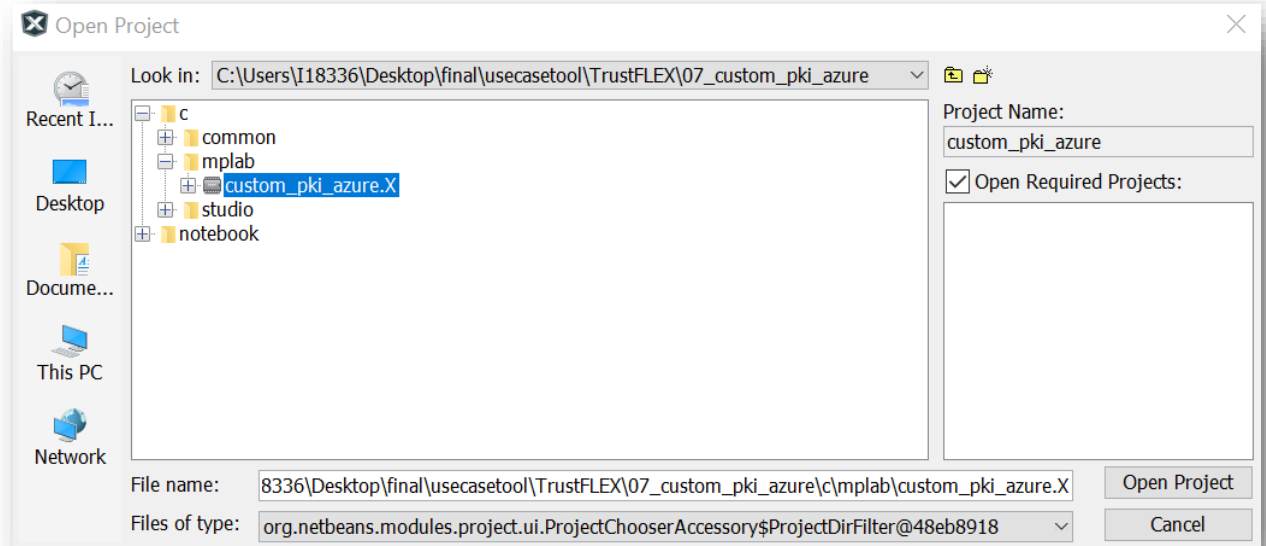
```
Attempting to connect to Azure IoT ...
  SSID:      karthi
  Password: karthikeyan
WINC1500 WIFI: Connected to the WIFI access point.
WINC1500 WIFI: Device IP Address: 192.168.119.192
WINC1500 WIFI: DNS lookup:
  Host:      trust-platform.azure-devices.net
  IP Address: 40.83.177.42
<APP><INFO>Socket 0 session ID = 1
SUCCESS: Azure Demo: Connected to Azure IoT.

SUCCESS: Subscribed to the MQTT update topic subscription:
SUCCESS: devices/0123A2682F50872801_ATECC/messages/devicebound/#

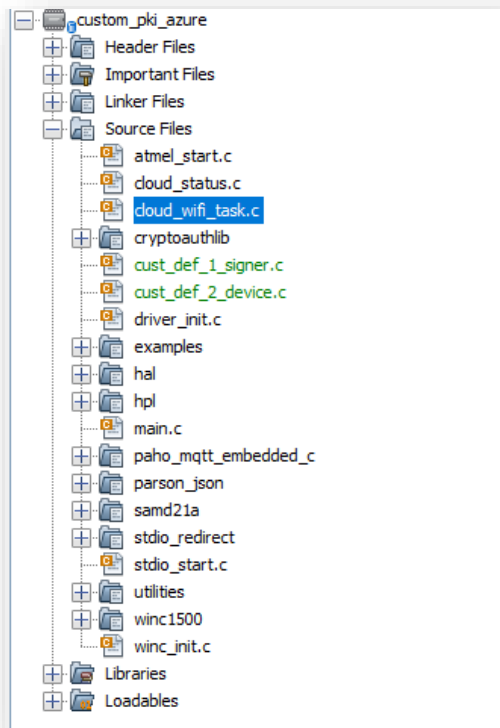
Publishing MQTT Shadow Update Message:
00000000 7B 22 6C 65 64 31 22 3A 22 6F 66 66 22 7D      {"led1":"off"}
```

#### 4.2.2 MPLAB:

1. Open **custom\_pki\_azure.X** project by navigating to MPLAB -> File -> Open Project  
-> **TrustFLEX\07\_custom\_pki\_azure\c\mplab\custom\_pki\_azure.X**



2. Open **cloud\_wifi\_task.c** file by navigating to **custom\_pki\_azure** -> **Source Files**  
-> **cloud\_wifi\_task.c**



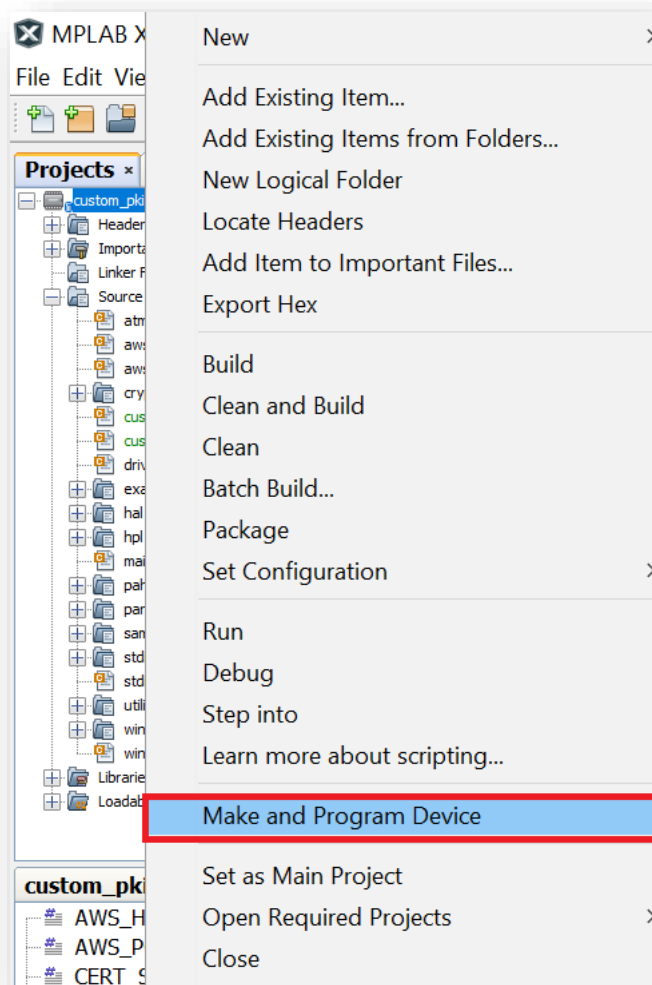
update the following constants before building the project:

- MAIN\_WLAN\_SSID
- MAIN\_WLAN\_PSK
- CLOUD\_ENDPOINT

The Highlighted area in CLOUD\_ENDPOINT string should have the Azure IOT Hub Name

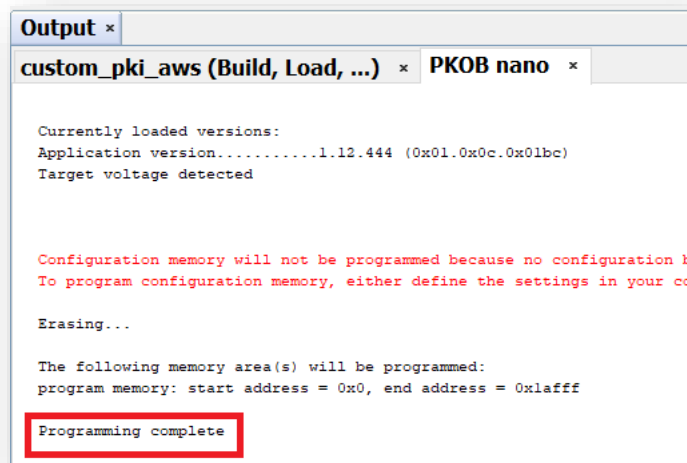
```
#define CLOUD_ENDPOINT "trust-platform.azure-devices.net"
```

3. Program the CryptoAuth Trust platform by navigating to **custom\_pki\_azure -> Make and Program Device**



This step may take some time, wait for MPLAB to program the device. Once it is done programming you will see "**Programming complete**" message in Output Window.





```
Output x
custom_pki_aws (Build, Load, ...) x PKOB nano x

Currently loaded versions:
Application version.....1.12.444 (0x01.0x0c.0x01bc)
Target voltage detected

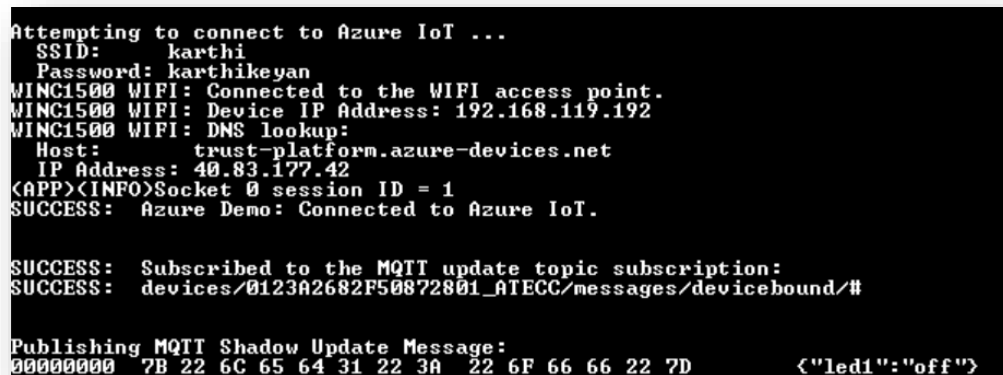
Configuration memory will not be programmed because no configuration b
To program configuration memory, either define the settings in your co

Erasing...

The following memory area(s) will be programmed:
program memory: start address = 0x0, end address = 0x1ffff

Programming complete
```

Once the programming is done, reset the hardware (press the reset button) and view the Console messages by using applications like 'Tera Term'. Open the application with the COM related to CryptoAuth Trust Platform with 115200-8-N-1 settings.



```
Attempting to connect to Azure IoT ...
SSID: karthi
Password: karthikeyan
WINC1500 WIFI: Connected to the WIFI access point.
WINC1500 WIFI: Device IP Address: 192.168.119.192
WINC1500 WIFI: DNS lookup:
Host: trust-platform.azure-devices.net
IP Address: 40.83.177.42
<APP><INFO>Socket 0 session ID = 1
SUCCESS: Azure Demo: Connected to Azure IoT.

SUCCESS: Subscribed to the MQTT update topic subscription:
SUCCESS: devices/0123A2682F50872801_ATECC/messages/devicebound/#

Publishing MQTT Shadow Update Message:
00000000 7B 22 6C 65 64 31 22 3A 22 6F 66 66 22 7D <"led1":"off">
```

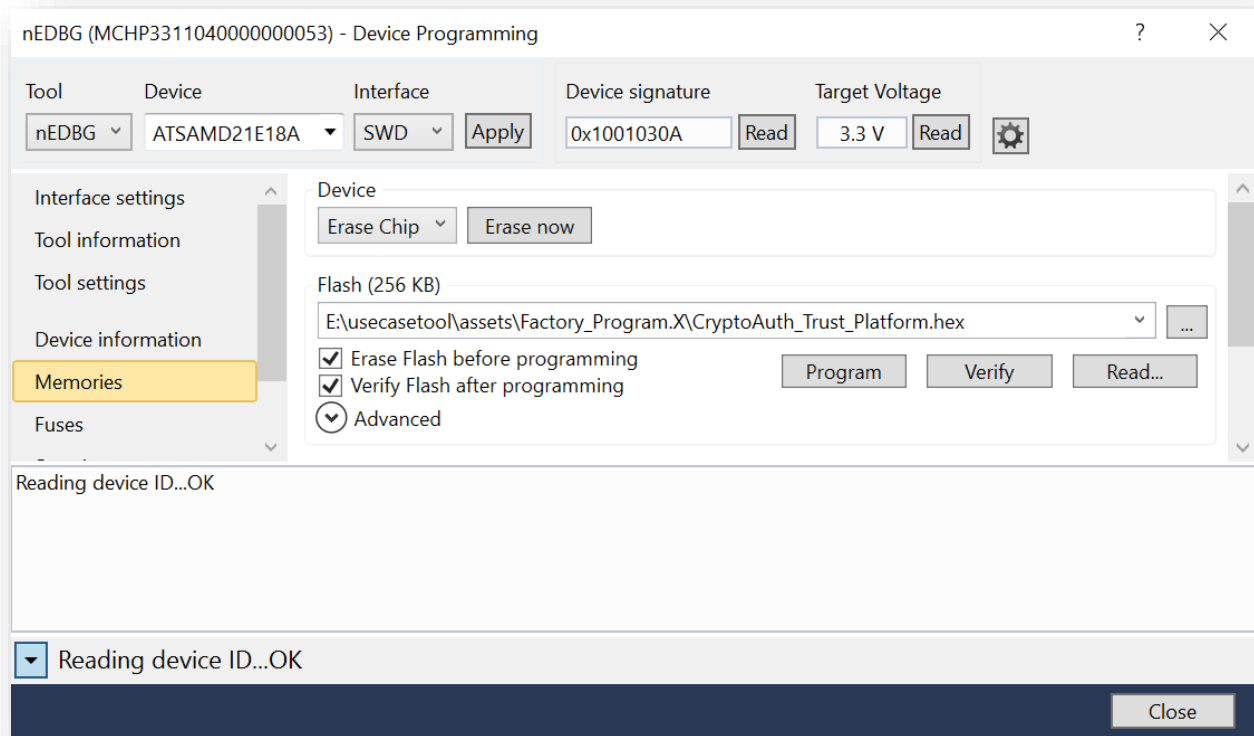
### 4.3 CryptoAuth Trust Platform Factory reset

If any embedded project is loaded to CryptoAuth Trust Platform, the default program that enables interaction with CryptoAuth Trust Platform tools will be erased.

Before using the CryptoAuth Trust Platform with any other notebook or tools on PC, its required to reprogram the default firmware. Default hex file is available at **assets\Factory\_Program.X\CryptoAuth\_Trust\_Platform.hex**

To reprogram using Atmel Studio:

1. Navigate to AtmelStudio -> Tools -> Device Programming
2. Select Tool as nEDBG and Apply
3. Go to Memories and navigate to above path under Flash dropdown
4. Check both Erase Flash and Verify Flash
5. Click on Program



To reprogram using MPLAB:

1. Open **assets\Factory\_Program.X** project in MPLAB IDE
2. Program the Crypto Trust platform by navigating to **CryptoAuth\_Trust\_Platform\_Factory\_Program -> Make and Program Device**

Now, CryptoAuth Trust Platform contains factory application that enables interactions with Notebooks and/or PC tools.

---

## 5 FAQ

### 1. What are the reasons for “**AssertionError: Can't connect to the USB dongle**” error?

There are many possibilities like,

1. Crypto Trust Platform is having different application than factory reset firmware. Refer to “CryptoAuth TrustPlatform Factory reset” section any usecase TrustFLEX Guide for reloading it
2. Check the switch positions on Crypto Trust Platform and/or ATECC608A Trust board
  - a. Correct Trust device should be connected and only one device of that type is allowed on the I2C bus. Multiple devices with same address results in error
3. Check USB connections to Crypto Trust Platform

### 2. How to reload factory default application to Crypto Trust Platform?

Refer to “CryptoAuth TrustPlatform Factory reset” section any usecase TrustFLEX Guide for reloading it.

### 3. Why does my C projects generates No such file or directory with ../../../../TFLXTLS\_resource\_generation/?

C project generates this error when the resources are not generated prior to using embedded projects. Running the resource generation notebook ensures these files and secrets are generated.

### 4. Before running any use case notebook and/or C project, why is it mandate to execute resource generation?

When resource generation notebook is executed, it generates and programs the required resources like secrets, keys and certificates. These are only prototyping keys and cannot be used for production. These keys will be used part of Usecase notebooks and C projects

### 5. How to know the resources being used in a use case?

Refer to individual Usecase description html for details on transaction diagrams, resources being used and other details. The resources required for given use case is mentioned in INFER CRYPTOGRAPHIC ASSETS section.

### 6. When should I select Custom certificates while doing resource generation?

Custom certificates are required when user wants to have their own root, signer instead of MCHP provided. The difference would be organization name, common name and validity are configurable

It is also possible to view the Console messages by using applications like TeraTerm. Open the application with the COM related to Crypto Trust Platform with 115200-8-N-1 settings

### 7. Why Azure demo application is not getting connected to cloud?

There are many possibilities like,

- a. Signer registration is not done to the account
- b. Device ID registration is not done to the account
- c. WiFi credentials are not populated or in correct in C project

- d. Azure IOT Hub name is not populated or in-correct in C project

---

## The Microchip Web Site

---

Microchip provides online support via our web site at <http://www.microchip.com/>. This web site is used as

a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

---

## Customer Change Notification Service

---

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at <http://www.microchip.com/>. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

---

## Customer Support

---

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support.

Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: <http://www.microchip.com/support>

---

## Microchip Devices Code Protection Feature

---

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the

operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.

- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

## Legal Notice

---

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

## Trademarks

---

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, Klear, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KlearNet, KlearNet logo, memBrain, Mindi, MiWi,

---

motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient

Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE,

Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2018, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN:

---

## Quality Management System Certified by DNV

---

### ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California

and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.



# Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
<b>Corporate Office</b> 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: <a href="http://www.microchip.com/support">http://www.microchip.com/support</a> Web Address: <a href="http://www.microchip.com">www.microchip.com</a> <b>Atlanta</b> Duluth, GA Tel: 678-975-9614 Fax: 678-957-1455 <b>Austin, TX</b> Tel: 512-257-3370 <b>Boston</b> Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 <b>Chicago</b> Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 <b>Dallas</b> Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 <b>Detroit</b> Novi, MI Tel: 248-848-4000 <b>Houston, TX</b> Tel: 281-894-5983 <b>Indianapolis</b> Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 <b>Los Angeles</b> Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 <b>Raleigh, NC</b> Tel: 919-844-7510 <b>New York, NY</b> Tel: 631-435-6000 <b>San Jose, CA</b> Tel: 408-735-9110 Tel: 408-436-4270 <b>Canada - Toronto</b> Tel: 905-695-1980 Fax: 905-695-2078	<b>Australia - Sydney</b> Tel: 61-2-9868-6733 <b>China - Beijing</b> Tel: 86-10-8569-7000 <b>China - Chengdu</b> Tel: 86-28-8665-5511 <b>China - Chongqing</b> Tel: 86-23-8980-9588 <b>China - Dongguan</b> Tel: 86-769-8702-9880 <b>China - Guangzhou</b> Tel: 86-20-8755-8029 <b>China - Hangzhou</b> Tel: 86-571-8792-8115 <b>China - Hong Kong SAR</b> Tel: 852-2943-5100 <b>China - Nanjing</b> Tel: 86-25-8473-2460 <b>China - Qingdao</b> Tel: 86-532-8502-7355 <b>China - Shanghai</b> Tel: 86-21-3326-8000 <b>China - Shenyang</b> Tel: 86-24-2334-2829 <b>China - Shenzhen</b> Tel: 86-755-8864-2200 <b>China - Suzhou</b> Tel: 86-186-6233-1526 <b>China - Wuhan</b> Tel: 86-27-5980-5300 <b>China - Xian</b> Tel: 86-29-8833-7252 <b>China - Xiamen</b> Tel: 86-592-2388138 <b>China - Zhuhai</b> Tel: 86-756-3210040	<b>India - Bangalore</b> Tel: 91-80-3090-4444 <b>India - New Delhi</b> Tel: 91-11-4160-8631 <b>India - Pune</b> Tel: 91-20-4121-0141 <b>Japan - Osaka</b> Tel: 81-6-6152-7160 <b>Japan - Tokyo</b> Tel: 81-3-6880-3770 <b>Korea - Daegu</b> Tel: 82-53-744-4301 <b>Korea - Seoul</b> Tel: 82-2-554-7200 <b>Malaysia - Kuala Lumpur</b> Tel: 60-3-7651-7906 <b>Malaysia - Penang</b> Tel: 60-4-227-8870 <b>Philippines - Manila</b> Tel: 63-2-634-9065 <b>Singapore</b> Tel: 65-6334-8870 <b>Taiwan - Hsin Chu</b> Tel: 886-3-577-8366 <b>Taiwan - Kaohsiung</b> Tel: 886-7-213-7830 <b>Taiwan - Taipei</b> Tel: 886-2-2508-8600 <b>Thailand - Bangkok</b> Tel: 66-2-694-1351 <b>Vietnam - Ho Chi Minh</b> Tel: 84-28-5448-2100	<b>Austria - Wels</b> Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 <b>Denmark - Copenhagen</b> Tel: 45-4450-2828 Fax: 45-4485-2829 <b>Finland - Espoo</b> Tel: 358-9-4520-820 <b>France - Paris</b> Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 <b>France - Saint Cloud</b> Tel: 33-1-30-60-70-00 <b>Germany - Garching</b> Tel: 49-8931-9700 <b>Germany - Haan</b> Tel: 49-2129-3766400 <b>Germany - Heilbronn</b> Tel: 49-7131-67-3636 <b>Germany - Karlsruhe</b> Tel: 49-721-625370 <b>Germany - Munich</b> Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 <b>Germany - Rosenheim</b> Tel: 49-8031-354-560 <b>Israel - Ra'anana</b> Tel: 972-9-744-7705 <b>Italy - Milan</b> Tel: 39-0331-742611 Fax: 39-0331-466781 <b>Italy - Padova</b> Tel: 39-049-7625286 <b>Netherlands - Drunen</b> Tel: 31-416-690399 Fax: 31-416-690340 <b>Norway - Trondheim</b> Tel: 47-7289-7561 <b>Poland - Warsaw</b> Tel: 48-22-3325737 <b>Romania - Bucharest</b> Tel: 40-21-407-87-50 <b>Spain - Madrid</b> Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 <b>Sweden - Gothenberg</b> Tel: 46-31-704-60-40 <b>Sweden - Stockholm</b> Tel: 46-8-5090-4654 <b>UK - Wokingham</b> Tel: 44-118-921-5800 Fax: 44-118-921-5820