

---

# TrustFLEX Step by Step Guide

## Firmware Validation

---

## Table of Contents

<b>1</b>	<b><i>Introduction</i></b> .....	<b>3</b>
1.1	<i>Getting started with Jupyter Notebook Tutorials</i> .....	3
1.1.1	Starting Jupyter Notebook.....	3
1.2	<i>Jupyter Notebook Basics</i> .....	4
1.2.1	The Notebook dashboard .....	4
1.3	<i>Introduction to Jupyter Notebook GUI</i> .....	4
<b>2</b>	<b><i>Jupyter Notebook Tutorials</i></b> .....	<b>6</b>
<b>3</b>	<b><i>Resource Generation Notebook</i></b> .....	<b>7</b>
<b>4</b>	<b><i>Use Case Prototyping</i></b> .....	<b>16</b>
4.1	<i>Running Firmware Validation example on Jupyter Notebook:</i> .....	16
4.2	<i>Running Firmware Validation on Embedded platform</i> .....	23
4.3	<i>Crypto Auth Trust Platform Factory reset</i> .....	25
<b>5</b>	<b><i>FAQ</i></b> .....	<b>26</b>

# 1 Introduction

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

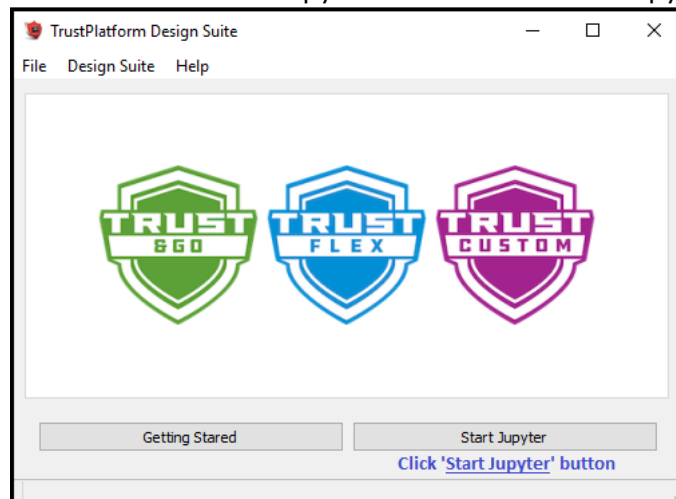
## 1.1 Getting started with Jupyter Notebook Tutorials

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 Trust Platform GUI Main window. Run START -> Trust Platform x.x.x icon. Click on 'Start Jupyter' button to launch Jupyter local server.



Clicking on Start Jupyter should be web browser tab like below,



## 1.2 Jupyter Notebook Basics

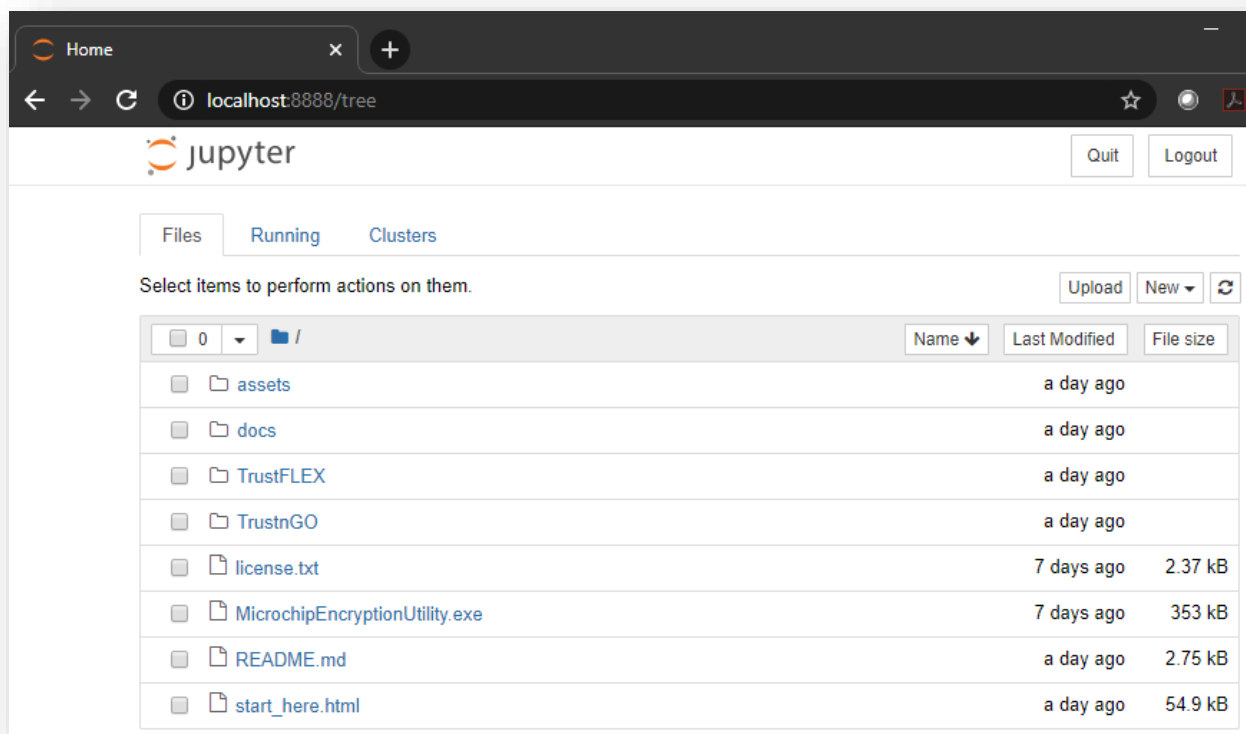
It is recommended to become familiar with Jupyter basic concepts with the online documentation, <https://jupyter-notebook.readthedocs.io/en/stable/examples/Notebook/Notebook%20Basics.html>

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 to the 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 on sub-directories in the notebook list, you can navigate your file system.

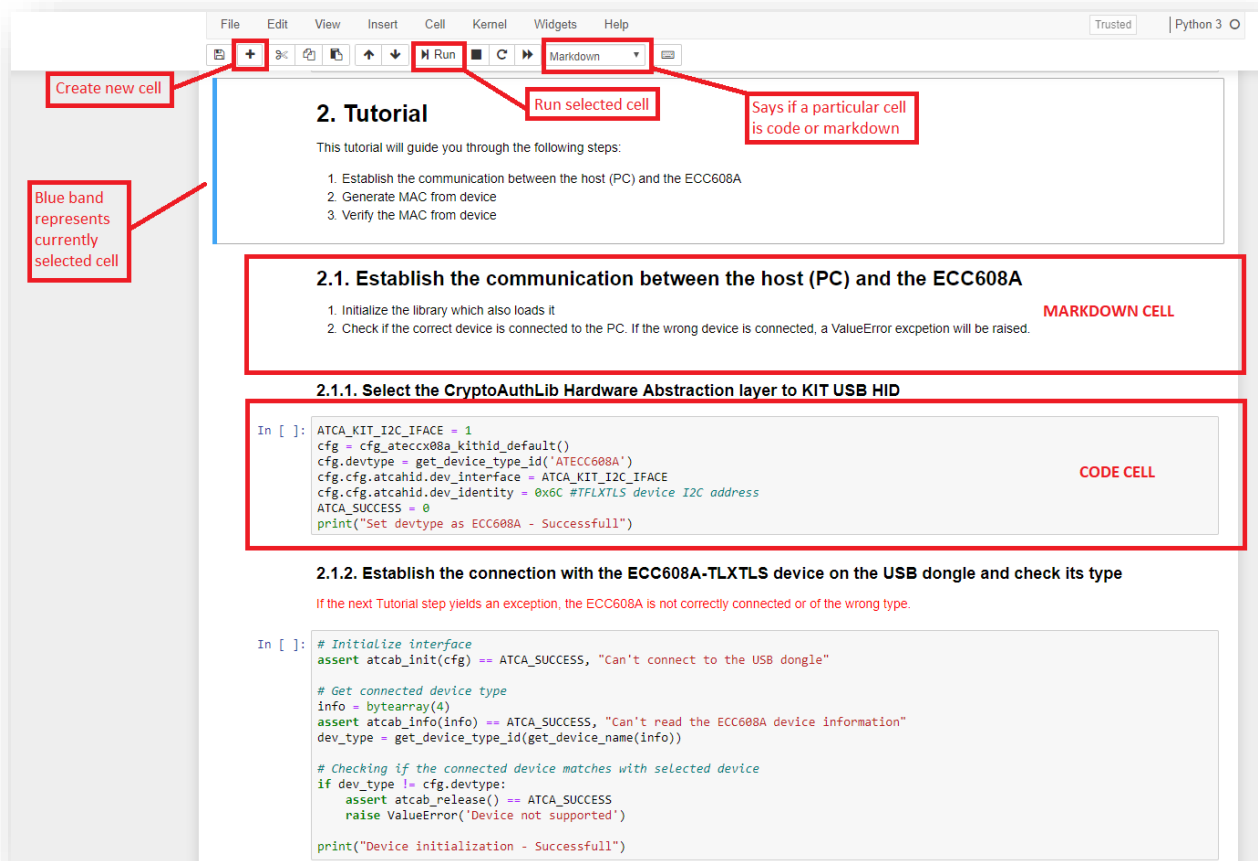


## 1.3 Introduction to Jupyter Notebook GUI.

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 to explain 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 Trust Platform Design Suite comes with Notebook Tutorials to easily prototype popular use cases for TrustFLEX. Here is the list of Jupyter Notebook Tutorials.

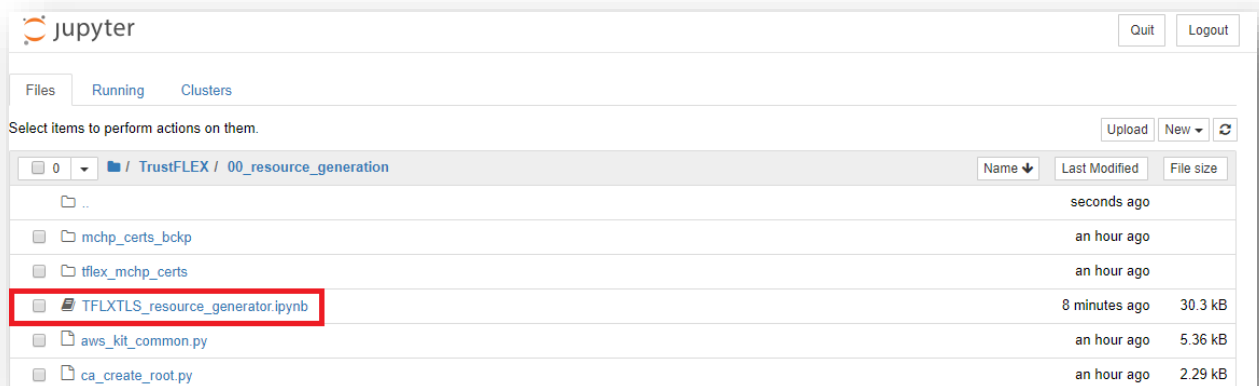
<b>Jupyter Notebook Tutorials</b>	<b>Relative Path</b>	<b>Applicable Devices</b>
Manifest Generation	TrustnGO\00_resource_generation\TNGTLS_manifest_file_generation.ipynb	Trust&GO
GCP Connect	TrustnGO\05_cloud_connect\notebook\gcp\TNGTLS_GCP_connect.ipynb	Trust&GO
AWS Connect	TrustnGO\05_cloud_connect\notebook\aws\TNGTLS_aws_connect.ipynb	Trust&GO
Azure Connect	TrustnGO\05_cloud_connect\notebook\azure\TNGTLS_azure_connect.ipynb	Trust&GO
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
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
Asymmetric authentication	08_asymmetric_authentication\notebook\TFLXTLS_asymmetric_authentication.ipynb	TrustFLEX
GCP Connect	TrustFLEX\10_cloud_connect\notebook\gcp\TFLXTLS_GCP_connect.ipynb	TrustFLEX
AWS Custom PKI	TrustFLEX\10_cloud_connect\notebook\aws\TFLXTLS_aws_connect.ipynb	TrustFLEX
Azure Connect	TrustFLEX\10_cloud_connect\notebook\azure\TFLXTLS_azure_connect.ipynb	TrustFLEX

### 3 Resource Generation Notebook

TFLXTLS device is one of the three devices available on Crypto Auth Trust Platform Development Kit. TrustFLEX devices come with pre-programmed 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 data in them.

The Resource Generator Notebook will create development keys and certificates for all slots that can be updated. Generated Keys and Certificate chains are stored in the PC file system. 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



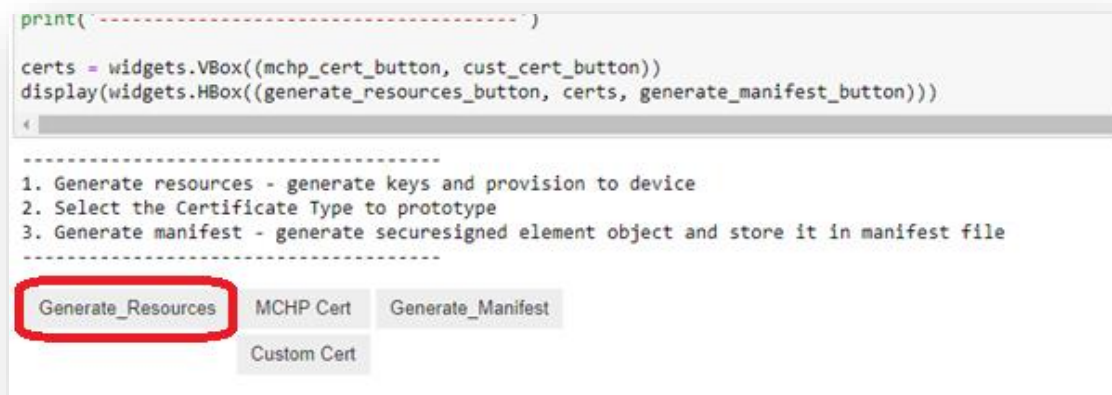
Run all cells of the Crypto Resource Generator Notebook: Kernel->Restart & Run All

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



Crypto Resource Generator notebook is common for all the use case which comes with option to load the signer certificate and device certificate. 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. Following are 3 different things can be performed,

#### 1. Generating resources to general key slots



The output log should resemble this:

-----  
Slot 0 is a private key slot, no action required  
Slot 1 is a private key slot, no action required  
Slot 2 is a private key slot, no action required  
Slot 3 is a private key slot, no action required  
Slot 4 is a private key slot, no action required



Slot 6 is a secret key, created slot\_6\_secret\_key.pem and programmed

NOTE: While writing symmetric key into secure element it has to be encrypted with IO protection key. So here, Slot 6 (IO protection key) is written before slot 5 (Symmetric key)

Slot 5 is a secret key, created slot\_5\_secret\_key.pem and programmed

Slot 7 is a secureboot digest slot, slot can only be written through secureboot command

Slot 8 is a general purpose slot of size 416 bytes, no action required

Slot 9 is a secret key, created slot\_9\_secret\_key.pem and programmed

Slot 10 is a certificate slot, no action required now, will be updated as part of Generate Certificates

Slot 11 is a certificate slot, no action required now, will be updated as part of Generate Certificates

Slot 12 is a certificate slot, no action required now, will be updated as part of Generate Certificates

Slot 13 is a public key slot, created slot\_13\_ecc\_key\_pair.pem and programmed

Slot 14 is a public key slot, created slot\_14\_ecc\_key\_pair.pem and programmed

Slot 15 is a public key slot, created slot\_15\_ecc\_key\_pair.pem and programmed

-----  
Key generation - Success  
-----

## 2. Generating MCHP or Custom Certificates

On selecting Custom certificates, it prompts 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.

- ```
-----
1. Generate resources - generate keys and provision to device
2. Select the Certificate Type to prototype
3. Generate manifest - generate securesigned element object and store it in manifest file
-----
```

```
Generate_Resources  MCHP Cert  Generate_Manifest
                     Custom Cert
```

```
-----
Slot 0 is a private key slot, no action required
Slot 1 is a private key slot, no action required
Slot 2 is a private key slot, no action required
Slot 3 is a private key slot, no action required
Slot 4 is a private key slot, no action required
Slot 6 is a secret key, created slot_6_secret_key.pem and programmed
```

NOTE: While writing symmetric key into secure element it has to be encrypted with IO protection key) is written before slot 5 (Symmetric key)

```
Slot 5 is a secret key, created slot_5_secret_key.pem and programmed
Slot 7 is a secureboot digest slot, slot can only be written through secureboot command
Slot 8 is a general purpose slot of size 416 bytes, no action required
Slot 9 is a secret key, created slot_9_secret_key.pem and programmed
Slot 10 is a certificate slot, no action required now, will be updated as part of Generate
Slot 11 is a certificate slot, no action required now, will be updated as part of Generate
Slot 12 is a certificate slot, no action required now, will be updated as part of Generate
Slot 13 is a public key slot, created slot_13_ecc_key_pair.pem and programmed
Slot 14 is a public key slot, created slot_14_ecc_key_pair.pem and programmed
Slot 15 is a public key slot, created slot_15_ecc_key_pair.pem and programmed
```

```
-----
Key generation - Success
-----
```

Org Name:

**Type Org Name and Press Enter to  
continue Custom Certs processing**

The output log should resemble this:

```
-----
Custom Certs processing...
Device contains custom device and signer certificates
Building new root certificate
Building new signer csr certificate
Building new signer certificate
Read device serial number...OK (SN: 01233E8A1491F2A601)
```

Read device public key from slot 0...OK (Public Key: CF1988BC3A6C252026FE70FB34397AD85A39AE811C722BFA6E5EC1E9CDA9133B3F0E91FD3877F25B8C893B311BAF0203CB5100C4CDABEBAFDAF3EBD550B00125)

Generating device certificate...OK (saved to device\_01233E8A1491F2A601.crt)

Saving signer certificate to device...OK

Saving device certificate to device...OK

Thing ID eabc56113c70227a18c0a62f7c285fc68d75f9cd

-----  
Custom certificate generation and provisioning - SUCCESS  
-----

Validate root certificate...OK

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

MIIByjCCAW+gAwIBAgIQeoueybRh8XWwzOkoixtW1jAKBggqhkJOPQQDAjA7MQ0wCwYDVQQKDAR0ZXN0MSowKAYDVQQDDCFDcnlwdG8gQXV0aGVudGljYXRpb24gUm9vdCBDQSAwMDIwIBcNMjAwNzAxMDgwNTE5WkgPMjA2MDA2MjEwODAxMTlaMDsxDTALBgNVBAoMBHRlc3QxKjAoBgNVBAMMIUNyeXB0byBBdXRoZW50aWNhdGlvbiBSb290IENBIDAwwMjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABFf6qcSyPv8iY0uccoTXSISstaz0ECCUxXUoqky8Xo40vsOCbPPt5QtlvNHnyy8tAbwza6DsAiz2sGLzDI5hQhqjUzBRMB0GA1UdDgQWBRRHVPQoljiq65JOG4vu5l32JzmkSTAfBgNVHSMEGDAWgBRHVPQoljiq65JOG4vu5l32JzmkSTAPBgNVHRMBAf8EBTADAQH/MAoGCCqGSM49BAMCA0kAMEYCIQCB7FKx5K33xK9E0PsWGKZRaaQxxSRypC66y4hVqWVmmMAIhAMIG22zNUKPHCcHQxfQssYH5LfR5SVE+WC3Hyxem/EVj

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

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

7a:8b:9e:c9:b4:61:f1:75:b0:cc:e9:28:8b:1b:56:d6

Signature Algorithm: ecdsa-with-SHA256

Issuer: O=test, CN=Crypto Authentication Root CA 002

Validity

Not Before: Jul 1 08:05:19 2020 GMT

Not After : Jun 21 08:05:19 2060 GMT

Subject: O=test, CN=Crypto Authentication Root CA 002

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:57:fa:a9:c4:b2:3e:ff:22:63:4b:9c:72:84:d7:

4a:54:ac:b5:ac:f4:10:20:94:c5:75:28:aa:4c:bc:

5e:8e:34:be:c3:82:6c:f3:ed:e5:0b:65:bc:d1:e7:

cb:2f:2d:01:bc:33:6b:a0:ec:02:2c:f6:b0:62:f3:  
0c:8e:61:42:1a  
ASN1 OID: prime256v1  
NIST CURVE: P-256  
X509v3 extensions:  
X509v3 Subject Key Identifier:  
47:54:F4:28:96:38:AA:EB:92:4E:1B:8B:EE:E6:5D:F6:27:39:A4:49  
X509v3 Authority Key Identifier:  
keyid:47:54:F4:28:96:38:AA:EB:92:4E:1B:8B:EE:E6:5D:F6:27:39:A4:49

X509v3 Basic Constraints: critical  
CA:TRUE

Signature Algorithm: ecdsa-with-SHA256  
30:46:02:21:00:81:ec:52:b1:e4:ad:f7:c4:af:44:d0:fb:16:  
18:a6:51:69:a4:31:c5:24:72:a4:2e:ba:cb:88:55:a9:65:66:  
30:02:21:00:c9:46:db:6c:cd:50:a3:c7:71:c1:d0:c5:f4:2c:  
b1:81:f9:2d:f4:79:49:51:3e:58:2d:c7:cb:17:a6:fc:45:63

Validate signer certificate...OK

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

MIIB3TCCAYKgAwIBAgIQV/RpeXxWfquIIYFCFTDc/TAKBggqhkJOPQQDAjA7MQ0w  
CwYDVQQKDAR0ZXN0MSowKAYDVQQDDCFDcnlwdG8gQXV0aGVudGljYXRpb24gUm9v  
dCBDQSAwMDIwIBcNMjAwNzAxMDgwMDAwWhgPMjA0MDA3MDEwODAwMDBaMDsxDTAL  
BgNVBAoMBHRlc3QxKjAoBgNVBAMMIUNyeXB0byBBdXR0ZW50aWNhdGlvb1BTaWdu  
ZXIgaRkZGRjBZMBMGBByqGSM49AgEGCCqGSM49AwEHA0IABCEubbOfXDakettxvfKu  
kfG5UhQNDHrPrZiURytSZmQ8p38VacZ682akSAC6XQYDzhly5/504eAHBCuN5rOt  
vnOjZjBkMA4GA1UdDwEB/wQEAwIBhjASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1Ud  
DgQWBBRycA/sc+NWXwp0wLudepyPtQtzFzAfBgNVHSMEGDAWgBRHVPQoljiq65JO  
G4vu5I32JzmkSTAKBggqhkJOPQQDAgNJADBGAiEA1ThacjiYboKYh69+NIIQKiX2  
wb7Jztq8zMsY61H/NKYCIQDQc2TQfOI9HBDUoDzUtTZNgIksElkU7ysiSgBhumAA  
zQ==

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

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

57:f4:69:79:7c:56:7e:ab:88:21:81:42:15:30:dc:fd

Signature Algorithm: ecdsa-with-SHA256

Issuer: O=test, CN=Crypto Authentication Root CA 002

Validity

Not Before: Jul 1 08:00:00 2020 GMT

Not After : Jul 1 08:00:00 2040 GMT

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

77:19:29:06:cc:14:4f:e7:b8:75:28:4b:ea:da:74:d2

Signature Algorithm: ecdsa-with-SHA256

Issuer: O=test, CN=Crypto Authentication Signer FFFF

Validity

Not Before: Jul 1 06:00:00 2020 GMT

Not After : Jul 1 06:00:00 2048 GMT

Subject: O=test, CN=sn01233E8A1491F2A601

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:cf:19:88:bc:3a:6c:25:20:26:fe:70:fb:34:39:

7a:d8:5a:39:ae:81:1c:72:2b:fa:6e:5e:c1:e9:cd:

a9:13:3b:3f:0e:91:fd:38:77:f2:5b:8c:89:3b:31:

1b:af:02:03:cb:51:00:c4:cd:ab:eb:af:da:f3:eb:

d5:50:b0:01:25

ASN1 OID: prime256v1

NIST CURVE: P-256

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Key Usage: critical

Digital Signature, Key Agreement

X509v3 Subject Key Identifier:

EA:BC:56:11:3C:70:22:7A:18:C0:A6:2F:7C:28:5F:C6:8D:75:F9:CD

X509v3 Authority Key Identifier:

keyid:72:70:0F:EC:73:E3:56:5F:0A:74:C0:BB:9D:7A:9C:8F:B5:0B:73:17

Signature Algorithm: ecdsa-with-SHA256

30:44:02:20:03:67:fd:0a:ea:c7:09:b0:ad:1b:2b:71:8c:90:

a5:62:74:a3:80:31:2f:31:a8:78:26:63:7c:9e:68:d0:50:1b:

02:20:45:9d:ee:bb:88:4c:ee:87:a7:6a:c2:b7:50:62:f8:01:

eb:ea:93:c5:f2:f2:7a:2d:64:c2:81:5c:7d:59:c7:bc

### 3. Generating Manifest file

```
-----  
1. Generate resources - generate keys and provision to device  
2. Select the Certificate Type to prototype  
3. Generate manifest - generate securesigned element object and store it in manifest file  
-----
```

Generate\_Resources

MCHP Cert

Generate\_Manifest

Custom Cert

The output log should resemble this:

```
-----  
Generating manifest data...OK (saved to TFLXTLS_devices_manifest.json)  
-----
```

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

After running this Notebook, it generates the required resources and program data zone with required secrets, keys and certificates. For this use case, IO protection key and firmware validation public key are loaded into TrustFLEX device in the slot 6 and 15 respectively.

## 4 Use Case Prototyping

This hands-on lab is intended to demonstrate the usage of TrustFLEX device to validate firmware that going to run on HostMCU. It uses asymmetric authentication.

To validate the firmware, following steps to be followed

1. Generating a firmware Signing Key pair
2. Signing the firmware
3. Updating the firmware to product
4. Verifying the firmware image

OEM to take care of first 2 things in a controlled environment. To have firmware validation functionality, once the firmware implementation is completed it should be signed by the OEM firmware signer to make the image authentic. Typically, OEM firmware signer's public key will be loaded to secure element and locked permanently.

On the product side, the digest and signature generated in the previous step will be provided to secure element using Secure boot command. Secure boot command will be executed on secure element with option to store (Full Copy) on successful validation of the digest and signature.

On TrustFLEX device secure boot configuration is set as "FullDig", which stores the firmware digest on the device (slot 7 on TrustFLEX). On subsequent boots, the digest is compared without ECC verify operations. While sending the digest to TrustFLEX device, the digest is encrypted with IO protection key to avoid man in the middle attack.

This lab is setup such a way firmware sign operation taken care by notebook, update and verify operations can be done both in notebook and embedded project. Firmware sign operations are NOT done in embedded project as it's the role of OEM but not the product.

The resource generation for TrustFLEX device will load

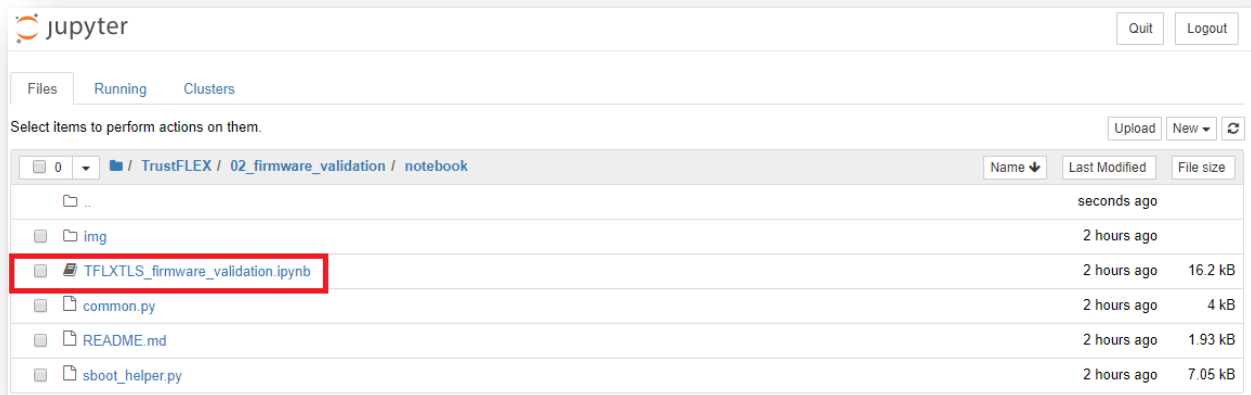
1. A prototyping firmware signing key
2. A prototyping IO protection key to Slot6
3. Signers public key to Slot15 respectively

Following sections provide detail steps to execute the Usecase both on Jupyter Notebook and on Embedded project

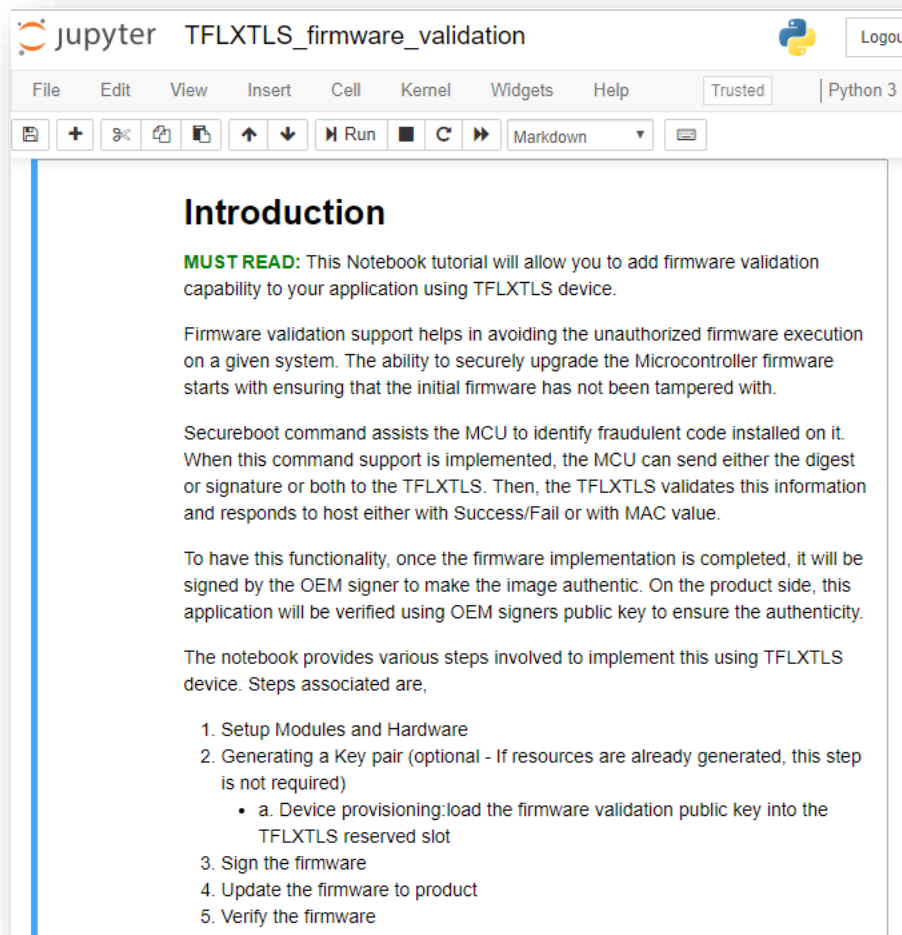
### 4.1 Running Firmware Validation example on Jupyter Notebook:

1. From the Jupyter Home page, navigate to **TrustFLEX\02\_firmware\_validation\notebook\TFLXTLS\_firmware\_validation.ipynb** notebook file and open it.

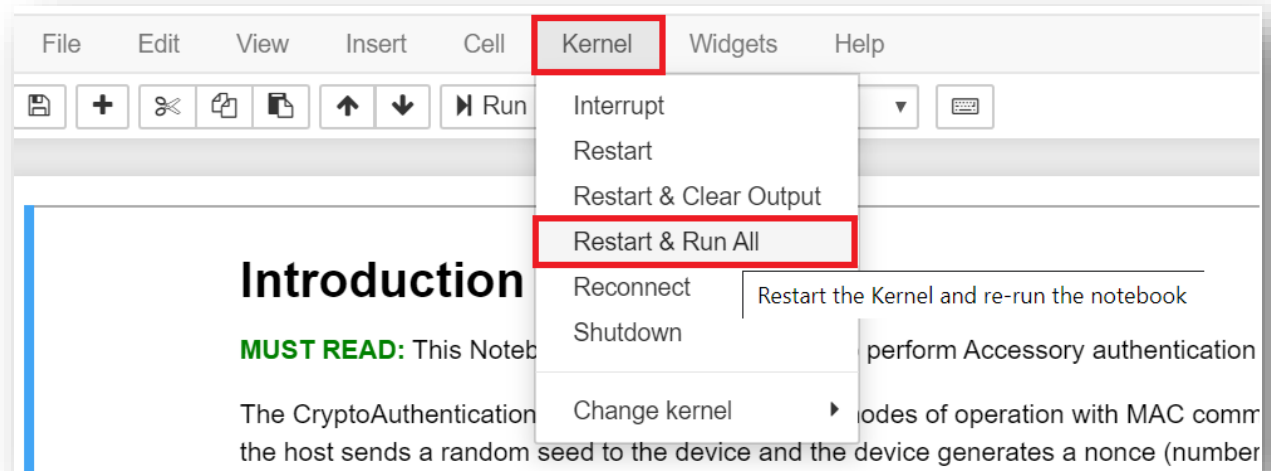




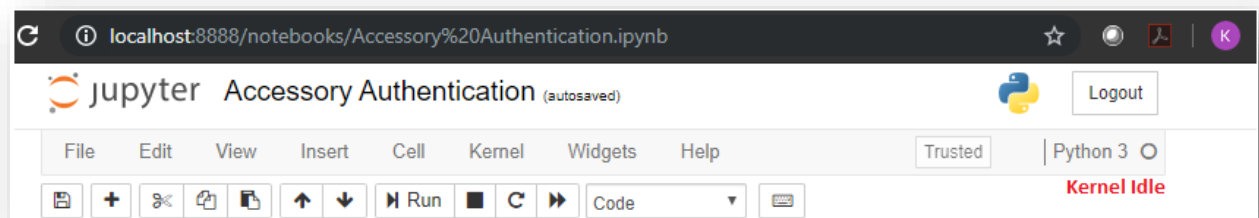
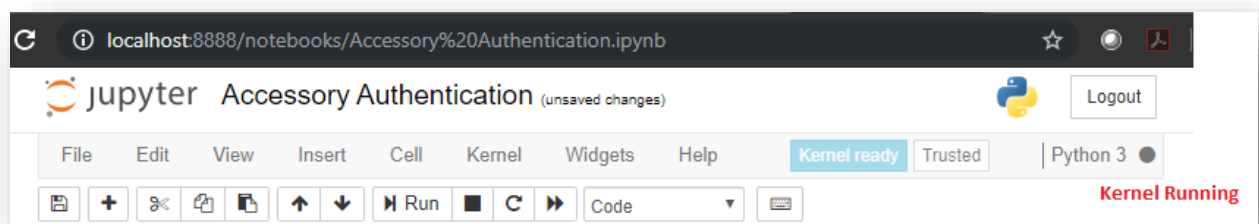
Opening the notebook from Jupyter home page should load the following on the browser,



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)



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

- There are 4 major steps in this lab

### **Generating a Firmware Validation key pair**

This step setups a temporary firmware signer to perform firmware validation process. This key generation is already taken care part of resource generation.

### **Sign the Firmware**

This step generates firmware digest by hash the example firmware image with SHA 256 algorithm and get it signed with firmware signer's private key. Then digest will

be encrypted with IO protection key to avoid man in the middle attack before host send digest to the device.

Here is how the memory of the Microcontroller is portioned. Microcontroller has a 256KB flash starting from 0x0000 0000, supporting address range from 0x0000 0000 to 0x0003 FFFF.

|                           |                            |
|---------------------------|----------------------------|
| Firmware validation image | 0x0000 0000 to 0x0000 BFFF |
| Application image         | 0x0000 C000 to 0x0003 FBFF |
| Signature data            | 0x0003 FC00 to 0x0003 FFFF |

The firmware validation image and the application image can be obtained by building (compile + link) the respective projects in the correct address spaces, the signature will be calculated and stitched with the other images through Jupyter Notebooks.

To get firmware validation hex, just navigate to

**TrustFLEX\02\_firmware\_validation\firmware.** Open either MPLAB project or Atmel studio project and build the project. After successful build, it will create .hex file under **TrustFLEX\02\_firmware\_validation\notebook\firm\_valid\*.hex.** We will be using this hex file in future steps.

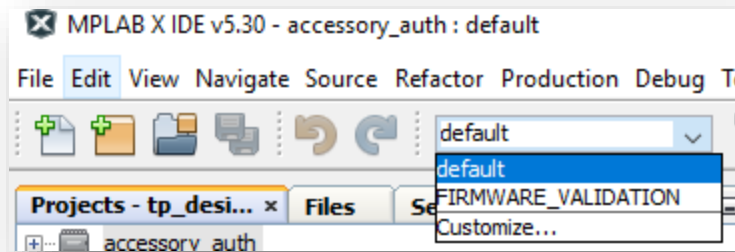
To get Application hex, open any of the use case example project either in MPLAB or Atmel studio. As discussed earlier, the application hex start address should be 0xC000. So, we need to change the build configuration to get output hex that starts from 0xC000.

The example applications in the DesignTools have two build configurations, one is **CONFIG\_STANDALONE/default** where application image starts from 0x00000000 and another one is

**CONFIG\_FIRMWARE\_VALIDATION/FIRMWARE\_VALIDATION** where application image starts from 0xC000. When Firmware validation feature is used, example application should be compiled using **CONFIG\_FIRMWARE\_VALIDATION/FIRMWARE\_VALIDATION** configuration.

MPLAB:

Let us use Accessory Authentication example as an application. To open project just navigate to **TrustFLEX\01\_accessory\_authentication\firmware** and select **accessory\_auth.X.**



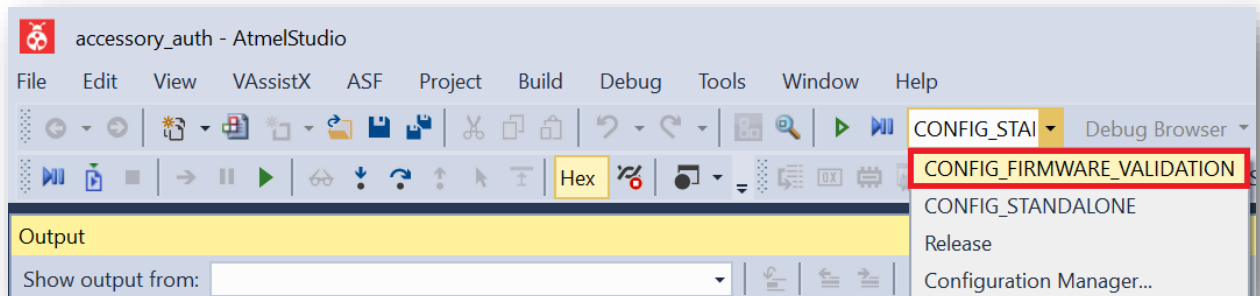
Here we need to select the FIRMWARE\_VALIDATION configuration to get application image start from 0xC000. Below screenshot display how to change the configuration, After changing the configuration, build the project. Once build successful, it will create .hex file under **TrustFLEX\02\_firmware\_validation\notebook\accessory\_auth\*.hex**.

**Note:** Before reusing the application in standalone mode this configuration should be set back to default.

ATMEL STUDIO: (Deprecated)

Let's use Accessory Authentication example as an application. To open project just navigate to **TrustFLEX\01\_accessory\_authentication\firmware\deprecated\_studio** and select **accessory\_auth.atsln**.

Here we need to select the CONFIG\_FIRMWARE\_VALIDATION configuration to get application image start from 0xC000. Below screenshot display how to change the configuration,



After changing the configuration, build the project. Once build is successful, it will create .hex file under **TrustFLEX\02\_firmware\_validation\notebook\accessory\_auth\*.hex**.

**Note:** Before reusing the application in standalone mode this configuration should be set back to CONFIG\_STANDALONE.

Now that we have all the binaries available, go back to the Firmware Validation Jupyter Notebook. Go to step 2.3, this step accepts two hex files, combines them and appends signature to it. Follow the below snapshots for reference. Make sure the correct images are selected on Upload buttons.

Load Hex files, Combine and Sign

```

In [4]: firmvalid_img_object = FileUpload(description='Step1a. Load Firmware Validation Hex', accept='*.hex', layout=widgets.Layout(width=200px, height=40px))
app_img_object = FileUpload(description='Step1b. Load Application Hex', accept='*.hex', layout=widgets.Layout(width='auto', height=40px))

def combine_hex(b):
    assert_msg = '''Its required both Firmware validation and Application hex files are selected before running this'''
    validity = any(firmvalid_img_object.value) & any(app_img_object.value)
    print('Upload Firmware validation and Application Hex file')
    display(widgets.Valid(value=validity, description='Upload'))
    assert validity, assert_msg
    combine_sign_hex(firmvalid_img_object, app_img_object)

tooltip = '''Combines both hex files and Signs the combined image, Should run only after loading both hex file'''
combine_and_sign = widgets.Button(description = "Step1c. Combine both HEX and Sign", tooltip=tooltip, layout=widgets.Layout(width=200px, height=40px))
combine_and_sign.on_click(combine_hex)
display(widgets.VBox((firmvalid_img_object, app_img_object, combine_and_sign)))

```

Step1a. Load Firmware Validation Hex (1)

Load Firmware Validation Hex file here

Step1b. Load Application Hex (1)

Load Application Hex file here

Step1c. Combine both HEX and Sign

Click this button to combine and Sign

Upload Firmware validation and Application Hex file

Upload

✓

Firmware validation binary size: 26468

Application binary size: 23768

Application digest:

70 58 09 D2 09 B3 9C D3 EA 6E CC 48 97 36 8C 19

1F 5B E1 7A D5 06 F6 13 67 F0 C5 D4 CD 0E A8 BB

Successfully Signed the firmware digest

Calculated signature:

0xC0, 0x88, 0x5E, 0xB8, 0x03, 0xA9, 0x5D, 0x11, 0x29, 0x7D, 0x21, 0x0F, 0x0A, 0x7F, 0x3D, 0x44,

0x07, 0x8F, 0xCB, 0xF7, 0x83, 0x09, 0xDD, 0xCB, 0xA3, 0x19, 0x91, 0xC2, 0xE5, 0xF4, 0x31, 0xE4,

0x29, 0x07, 0xA1, 0x63, 0xF8, 0x9C, 0xCE, 0x91, 0x2D, 0x2B, 0x58, 0x42, 0x06, 0x3F, 0xC0, 0x3D,

0x37, 0x47, 0x23, 0x12, 0xDF, 0x7D, 0xDA, 0x2B, 0xC8, 0xDB, 0x4A, 0x5D, 0x69, 0x5E, 0xE9, 0xA4,

“Combine HEX” will combine the firmware validation hex, accessory auth hex and will append the signature to it. The combined hex file will be store in the PC at DesignTool\ TrustFLEX\02\_firmware\_validation\notebook \combined\_image.hex

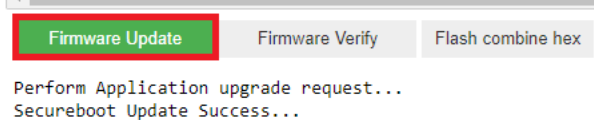
At this step, we have the combined image available for firmware validation update and verify operations. Both update and verify can be performed on the Notebook itself or on embedded projects.

## Update the firmware to product

Before verifying the firmware’s validity, the firmware digest should be verified and stored to secure element. In this step host sends the encrypted firmware digest and signature to device to validate the firmware. Here the firmware is validated by verifying the signature using firmware signer’s public key. Upon successful validation, the device stores the digest to Secureboot digest slot i.e. slot7.

```
# Perform Secureboot operation on the application file
print('Perform Application validation request... ')
assert atcab_secureboot_mac(SECUREBOOT_MODE_FULL_STORE, digest, signature,
if 1 == bool(is_verified.value):
    print('Secureboot Verify Success...')
    firmware_verify.button_style = 'success'
else:
    firmware_verify.button_style = 'danger'
    print('Secureboot Verify failed...')

firmware_update.on_click(secureboot_update)
firmware_verify.on_click(secureboot_verify)
display(widgets.HBox((firmware_update, firmware_verify, flash_hex)))
```



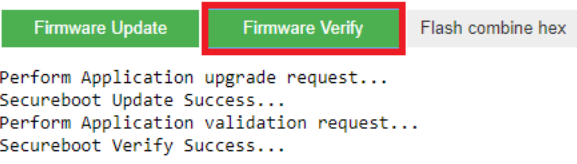
Clicking on “**Firmware Update**” will perform the above steps between host (PC) and the TrustFLEX device. Once firmware update is completed successfully, current firmware digest will be stored in the Secureboot digest slot.

### Verifying the firmware image

This step recalculates the digest from the example bin (secureboot\_test\_app.bin). The encrypted digest will be sent to TrustFLEX. Upon successful validation, the device returns MAC value corresponding to this verify request.

```
is_verified = atcab_secureboot_mac(SECUREBOOT_MODE_FULL_STORE, digest, signature, host_random,
# Perform Secureboot operation on the application file
print('Perform Application validation request... ')
assert atcab_secureboot_mac(SECUREBOOT_MODE_FULL_STORE, digest, signature, host_random,
if 1 == bool(is_verified.value):
    print('Secureboot Verify Success...')
    firmware_verify.button_style = 'success'
else:
    firmware_verify.button_style = 'danger'
    print('Secureboot Verify failed...')

firmware_update.on_click(secureboot_update)
firmware_verify.on_click(secureboot_verify)
display(widgets.HBox((firmware_update, firmware_verify, flash_hex)))
```



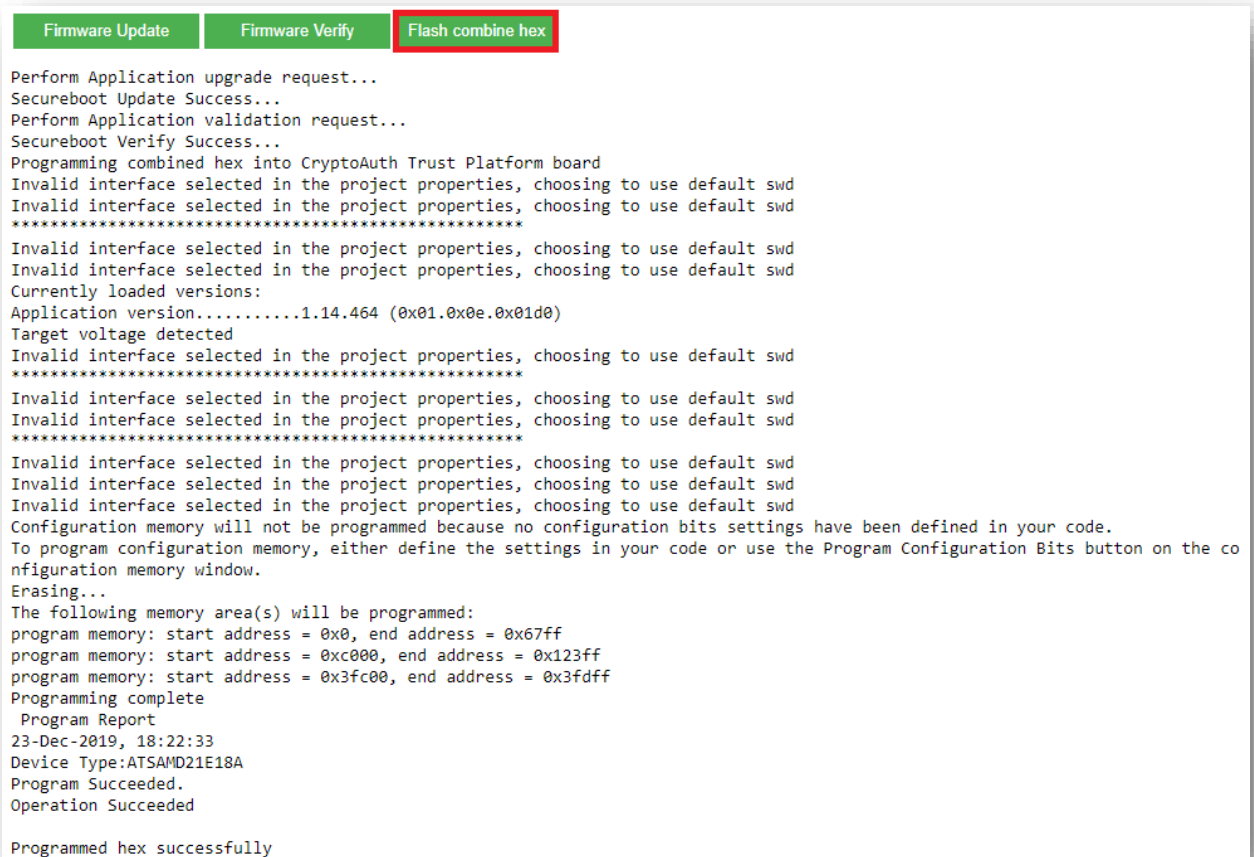
Clicking on “**Firmware Verify**” will perform the above steps between host (PC) and the TrustFLEX device.

Pressing "Firmware Update" and "Firmware Verify" should turn to green to indicate successful firmware update and verify operations.

### Flash Combine Hex

This step programs the Crypto Auth Trust Platform with combined hex (combined\_image.hex) using MPLABX IPE. To use this option, its required to provide MPLAB X IDE path in Trust Platform GUI -> Settings -> MPLAB X IDE.

Clicking on "Flash combine hex" will program Crypto Auth Trust Platform with combined hex.



```
Perform Application upgrade request...
Secureboot Update Success...
Perform Application validation request...
Secureboot Verify Success...
Programming combined hex into CryptoAuth Trust Platform board
Invalid interface selected in the project properties, choosing to use default swd
Invalid interface selected in the project properties, choosing to use default swd
*****
Invalid interface selected in the project properties, choosing to use default swd
Invalid interface selected in the project properties, choosing to use default swd
Currently loaded versions:
Application version.....1.14.464 (0x01.0x0e.0x01d0)
Target voltage detected
Invalid interface selected in the project properties, choosing to use default swd
*****
Invalid interface selected in the project properties, choosing to use default swd
Invalid interface selected in the project properties, choosing to use default swd
*****
Invalid interface selected in the project properties, choosing to use default swd
Invalid interface selected in the project properties, choosing to use default swd
Invalid interface selected in the project properties, choosing to use default swd
Configuration memory will not be programmed because no configuration bits settings have been defined in your code.
To program configuration memory, either define the settings in your code or use the Program Configuration Bits button on the co
nfiguration memory window.
Erasing...
The following memory area(s) will be programmed:
program memory: start address = 0x0, end address = 0x67ff
program memory: start address = 0xc000, end address = 0x123ff
program memory: start address = 0x3fc00, end address = 0x3fdff
Programming complete
Program Report
23-Dec-2019, 18:22:33
Device Type:ATSAMD21E18A
Program Succeeded.
Operation Succeeded

Programmed hex successfully
```

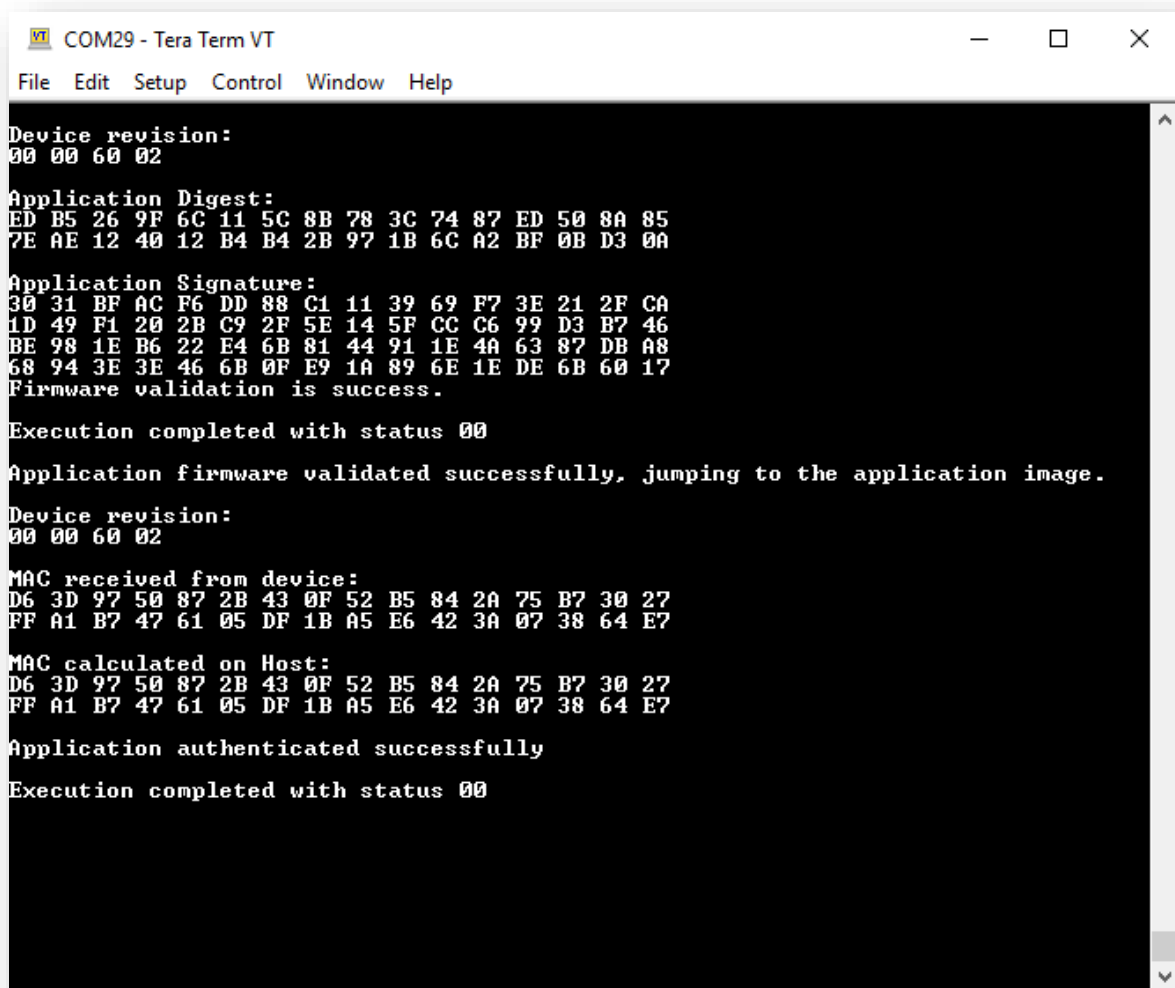
Pressing "Flash combine hex" should turn green to indicate that, it programmed combined hex successfully.

This requires MPLAB X IDE path to be set on GUI. To program this Crypto Auth Trust Platform manually refer

## 4.2 Running Firmware Validation on Embedded platform

The program output can be viewed using a serial terminal. Terminal needs to be opened with 115200-8-N-1 settings.

Output on the serial terminal would look like the image below,



```
COM29 - Tera Term VT
File Edit Setup Control Window Help

Device revision:
00 00 60 02

Application Digest:
ED B5 26 9F 6C 11 5C 8B 78 3C 74 87 ED 50 8A 85
7E AE 12 40 12 B4 B4 2B 97 1B 6C A2 BF 0B D3 0A

Application Signature:
30 31 BF AC F6 DD 88 C1 11 39 69 F7 3E 21 2F CA
1D 49 F1 20 2B C9 2F 5E 14 5F CC C6 99 D3 B7 46
BE 98 1E B6 22 E4 6B 81 44 91 1E 4A 63 87 DB A8
68 94 3E 3E 46 6B 0F E9 1A 89 6E 1E DE 6B 60 17
Firmware validation is success.

Execution completed with status 00

Application firmware validated successfully, jumping to the application image.

Device revision:
00 00 60 02

MAC received from device:
D6 3D 97 50 87 2B 43 0F 52 B5 84 2A 75 B7 30 27
FF A1 B7 47 61 05 DF 1B A5 E6 42 3A 07 38 64 E7

MAC calculated on Host:
D6 3D 97 50 87 2B 43 0F 52 B5 84 2A 75 B7 30 27
FF A1 B7 47 61 05 DF 1B A5 E6 42 3A 07 38 64 E7

Application authenticated successfully

Execution completed with status 00
```

On any error, LED blinks five times every second.



### 4.3 Crypto Auth Trust Platform Factory reset

Once any of the embedded project is loaded to Crypto Auth Trust Platform, the default program that enables interaction with Trust Platform tools will be erased.

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

If Trust Platform GUI is provided with MPLAB X IDE installation location, notebooks can program the Factory reset hex file if its not available by default.

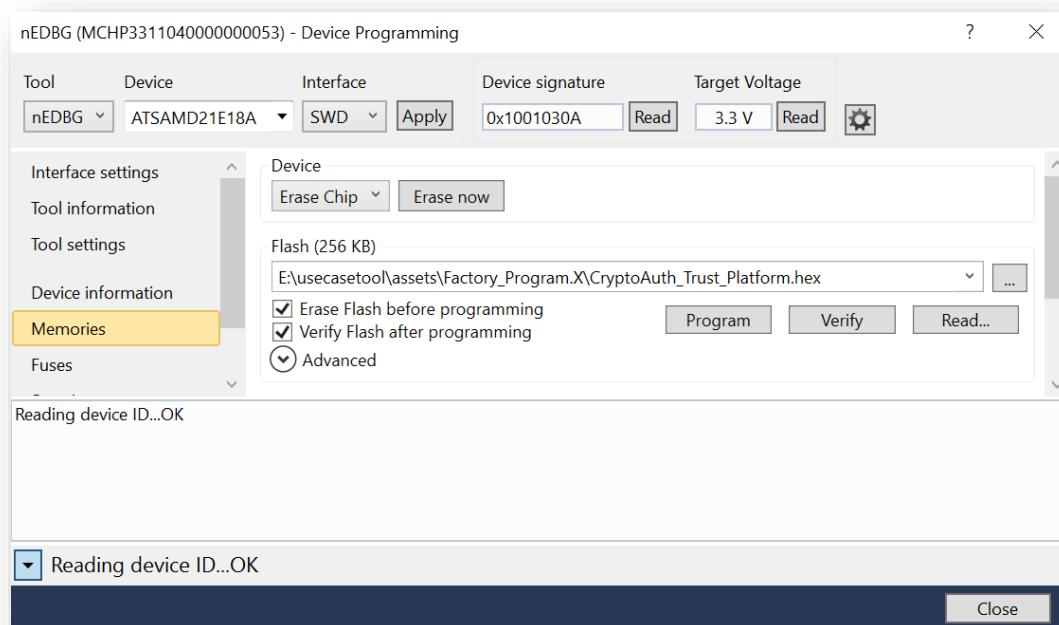
This can also be done manually by MPLAB and Atmel Studio

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**

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



Now, Crypto Auth Trust Platform contains factory programmed 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 “Crypto Auth Trust Platform Factory reset” section any usecase TrustFLEX Guide for reloading it
2. Check the switch positions on Crypto Trust Platform and/or ATECC608B 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 “Crypto Auth Trust Platform Factory reset” section any usecase TrustFLEX Guide for reloading it.

### 3. Why does my C projects generates No such file or directory with `../..../00_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

### 7. How to know whether C project is executing on Trust Platform or not after programming?

Once the programming is done, the firmware will do use case operation. Depending on the use case operation’s output, the Crypto Trust Platform board’s status LED will blink at different rates.

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

**8. Why is firmware validation project fails with error “Firmware validation is failed! with status 01”?**

There are many possibilities like,

- a. The resources on TrustFLEX device and on the host (PC) could be different. Rerun “Resource Generation Notebook” section for reloading it.
- b. Firmware digest is not matched. Make sure that firmware Update step is executed using Notebook prior to running 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,

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