

TA010 Asymmetric Authentication

TPDS Usecase Guide

Table of Contents

TA010 Asymmetric Authentication	3
Description	3
Training Video	4
TA010 Asymmetric Authentication	4
Prerequisites	4
Setting up Cryptoauth Trust Platform Development Kit (DM320118)	4
Setting up for Usecase.....	5
Opening the TA010 Asymmetric Authentication Usecase.....	6
Provisioning Blank TA010 Device	7
Open TA010-TFLXAUTH Configurator.....	7
Provisioning Usecase Resources	9
Build and Program Application	12
Conclusion	15
Microchip Information	16
The Microchip Website	16
Product Change Notification Service	16
Customer Support.....	16
Microchip Devices Code Protection Feature	16
Legal Notice	17
Trademarks	17
Quality Management System.....	18

TA010 Asymmetric Authentication

Asymmetric Authentication in computer security involves two entities exchanging information to verify each other's identity. This process aims to prevent cloning and counterfeiting, ensuring that an object is genuine and authorized to connect to a product. This example demonstrates the use of asymmetric authentication with the Microchip TA010-TFLXAUTH device for accessory or disposable authentication. It details how the Microchip TA010-TFLXAUTH device can be used for asymmetric authentication through device certificates and ECC key pairs.

Description

- Implements a comprehensive asymmetric (public/private) key cryptographic signature solution based on Elliptic Curve Cryptography (ECC) and the ECDSA signature protocol.
- **Verify Certificate Chain:**
 - The Host requests the Signer Certificate and verifies the certificate with the Authority Public key(Root).
 - Upon successful verification, the Host requests the Device Certificate and verifies it using the Signer Certificate.
- **Challenge-Response:**
 - The Host generates a random number challenge and sends it to the TA010-TFLXAUTH.
 - The TA010-TFLXAUTH signs the random number challenge with the Device Private Key.
 - The signed challenge is returned to the Host for verification using the Device Public Key, thereby completing the Chain of Trust verification.
 - In this usecase, ATECC608 is used for Certificate chain verification and signature verification on Host side.

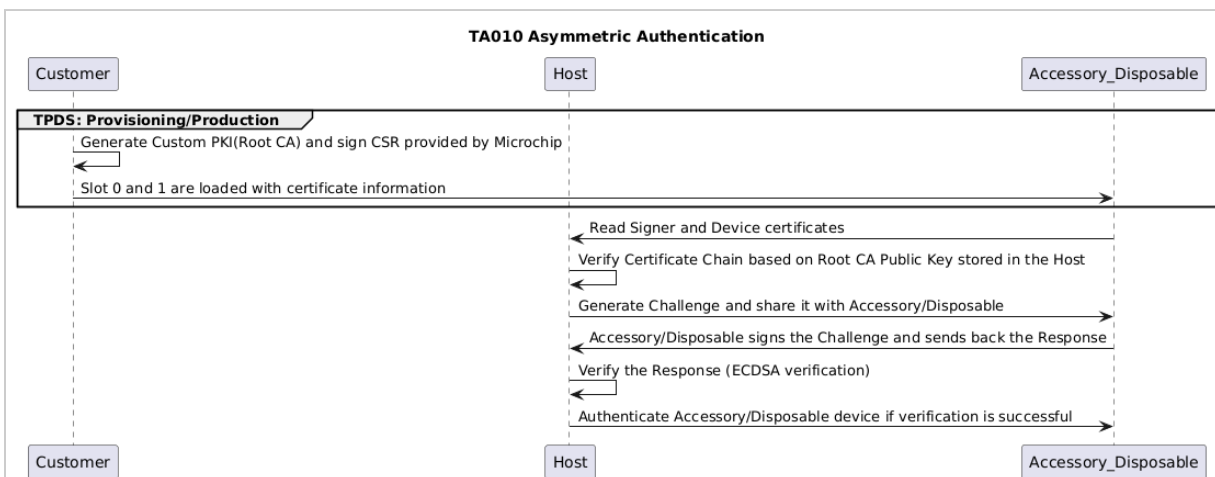


Figure-1

Training Video



Figure-2

TA010 Asymmetric Authentication

Prerequisites

- [TPDS\(Trust Platform Design Suite\)](#)
- [MPLAB® X IDE](#)
- [Cryptoauth Trust Platform Development Kit](#)
- [EV74C12A - TA010 mikroBUS Evaluation Board](#)

Setting up Cryptoauth Trust Platform Development Kit (DM320118)

- Ensure both the ON switch and CTS switch on the DM320118 Kit is in the ON position. Refer to label 6 in the figure below.

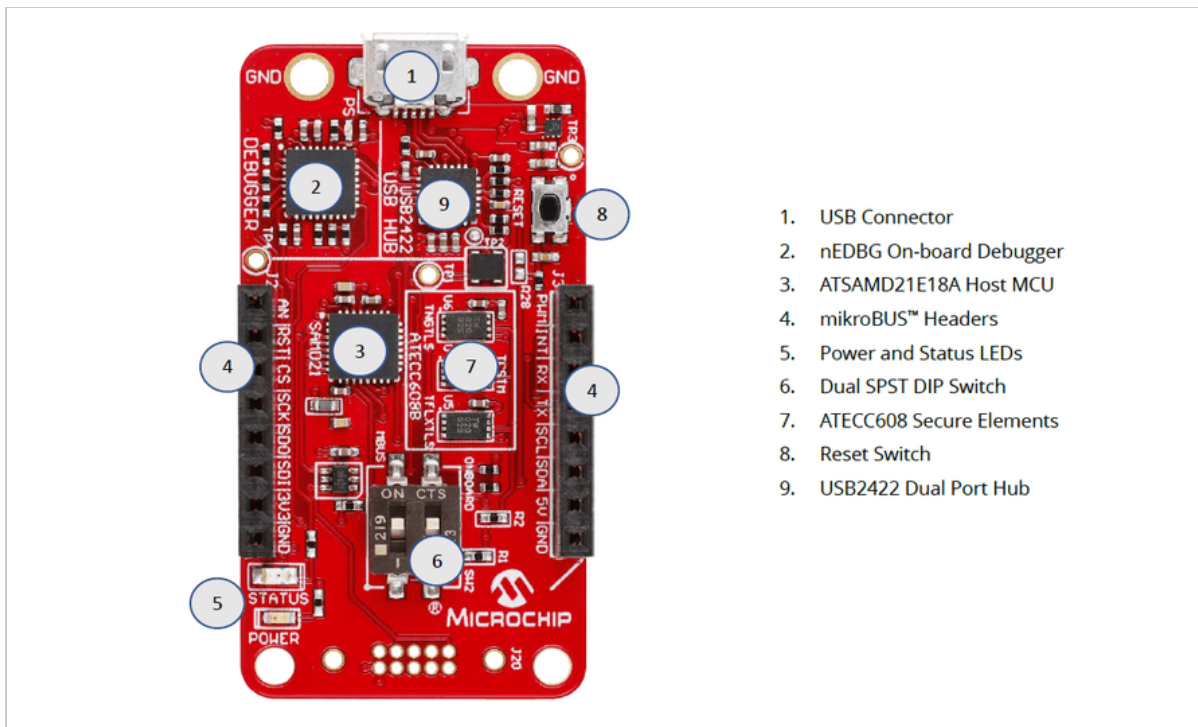


Figure-3

- Insert the EV74C12A Socket Board into the mikroBUS header of the Cryptoauth Trust Platform Development Kit.
- Connect the micro USB port on the board to the computer using a micro USB cable. You should notice Power LEDs light up on both the Trust Platform board as well as the EV74C12A Socket board.

Setting up for Usecase

- Make sure the MPLABX path is set in File -> Preferences -> MPLABX path.

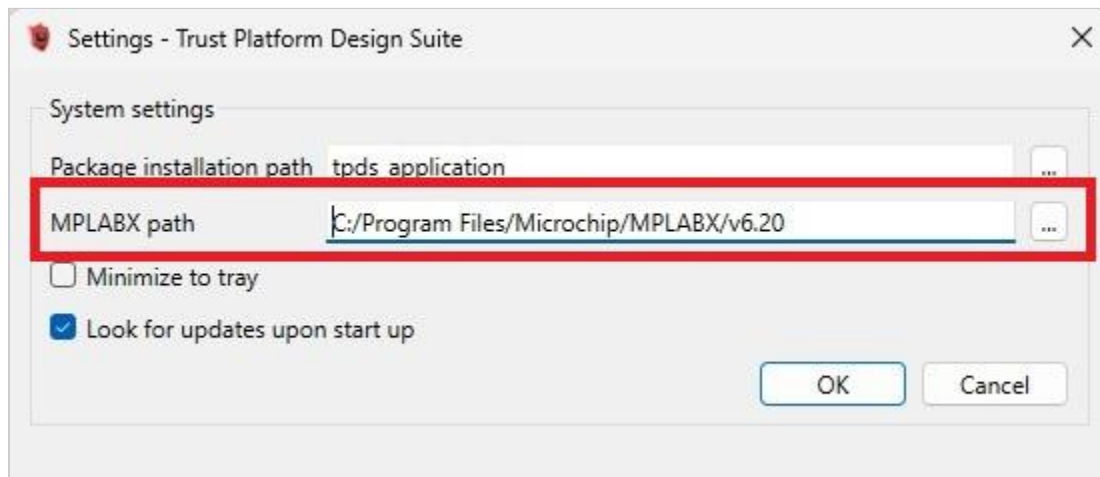


Figure-4

- Make sure the DM320118 board is factory programmed. Navigate to the Utilities Tab, select **DM320118** and press **Factory Program**. This step ensures the MCU is programmed with the

default firmware needed to provision the TA010 in the next steps. Without the default firmware, the next steps will not work.

- After factory programming process is complete, launch the Terminal application (e.g., Tera Term) on your computer.
- Connect to the Virtual COM port and configure the serial settings as follows:
 - Baud : 115200
 - Data : 8 Bits
 - Parity : None
 - Stop : 1 Bit
 - Flow Control : None
- Press the Reset button on the Cryptoauth Trust Platform Development Kit and observe a similar log:

```
-- CryptoAuth Trust Platform(DM320118) --
-- Compiled: Jun  1 2023 08:10:49 v1.1.0 --
-- Console log (115200-8-N-1) --

KitParser Version: v3.2.0

Device Discovery.....
I2C ECC608B  C0
I2C TA010   70
I2C ECC608B  6C
I2C ECC608B  6A
I2C TA100   2E
SPI TA100
SWI TA010   72
Completed
```

Figure-5

Opening the TA010 Asymmetric Authentication Usecase

- Open TPDS and navigate to Usecases Section.
- Select Usecase as **Asymmetric Authentication** under TA010-TFLXAUTH and the kit as **CryptoAuth Trust Platform**

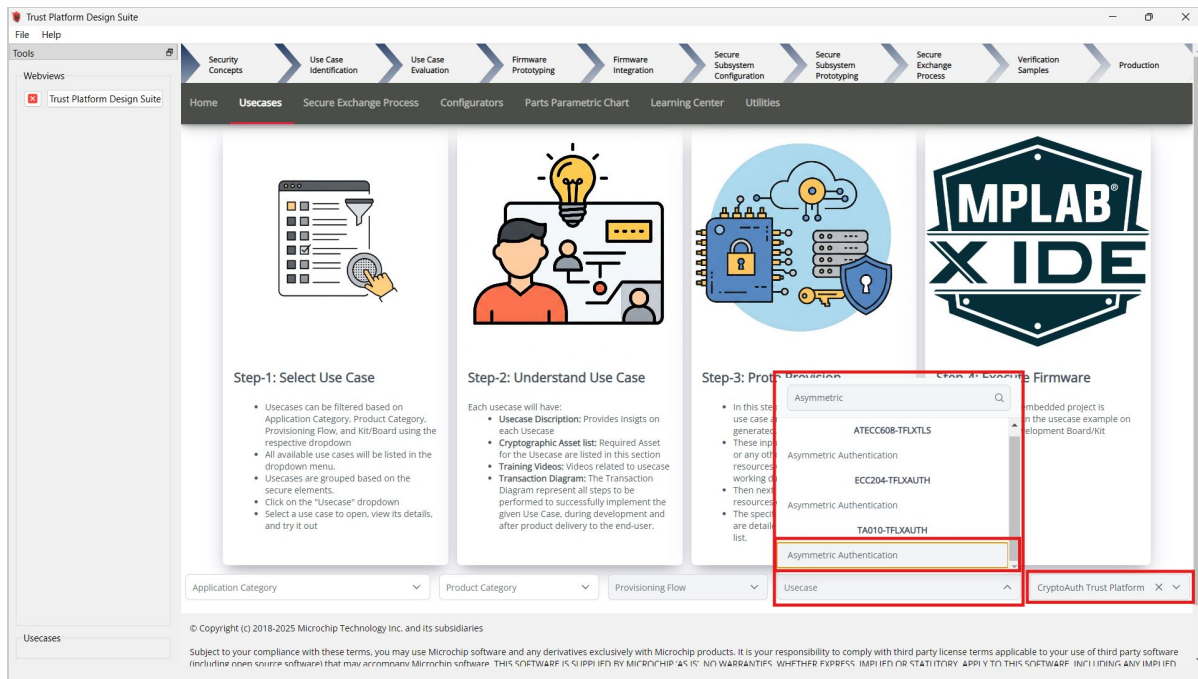


Figure-6

- The TA010-TFLXAUTH - Asymmetric Authentication usecase will open as below:

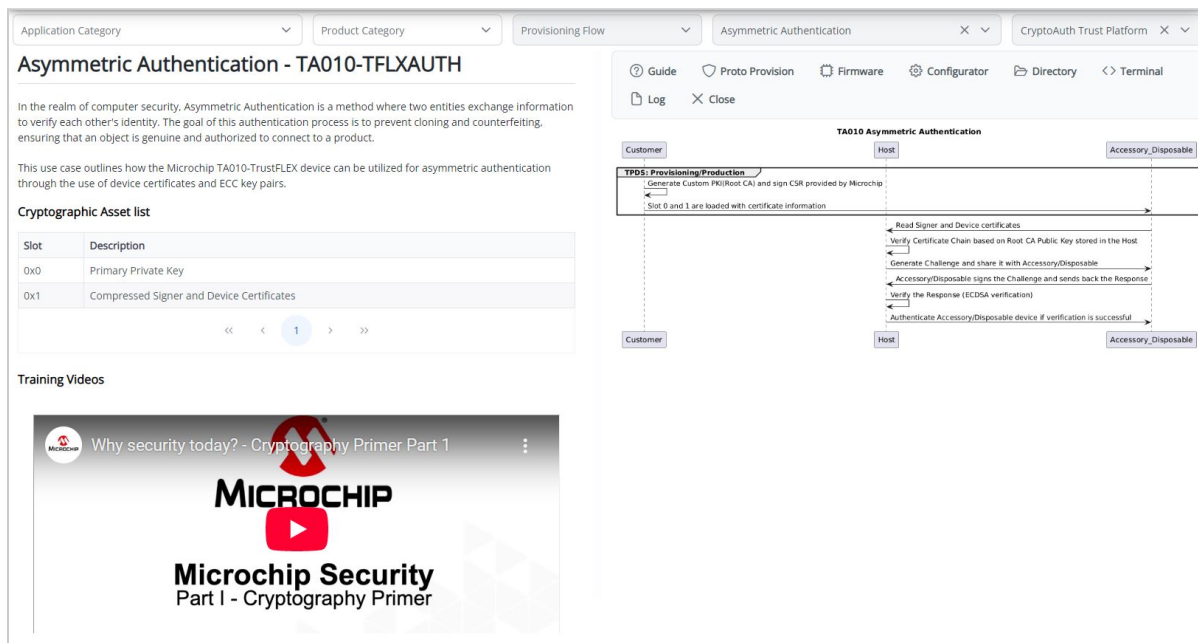


Figure-7

Provisioning Blank TA010 Device

To configure a blank TA010 device into TA010-TFLXAUTH device for the usecases, follow these steps:

Open TA010-TFLXAUTH Configurator

Click on the "Configurator" button within the use case to launch the TA010-TFLXAUTH Configurator.

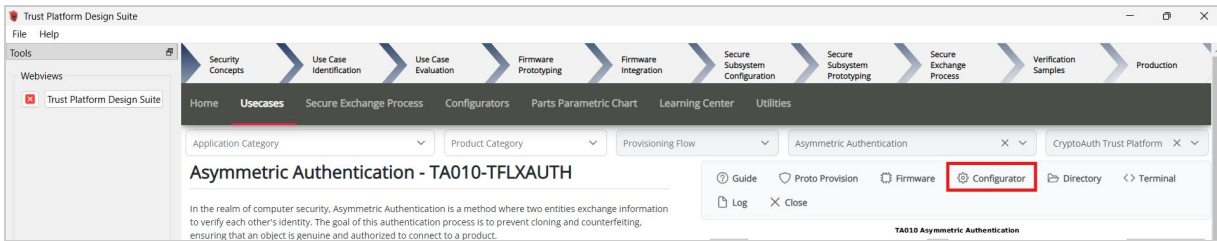


Figure-8

Adjust the Configuration

Once the TA010-TFLXAUTH Configurator is open:

- Leave the Device address empty to configure with the default TFLXAUTH address. **The use case requires the device to be configured with the default TFLXAUTH address.**
- Select the I2C or SWI interface in the configurator based on the interface of the device.
- Select Limited key use.

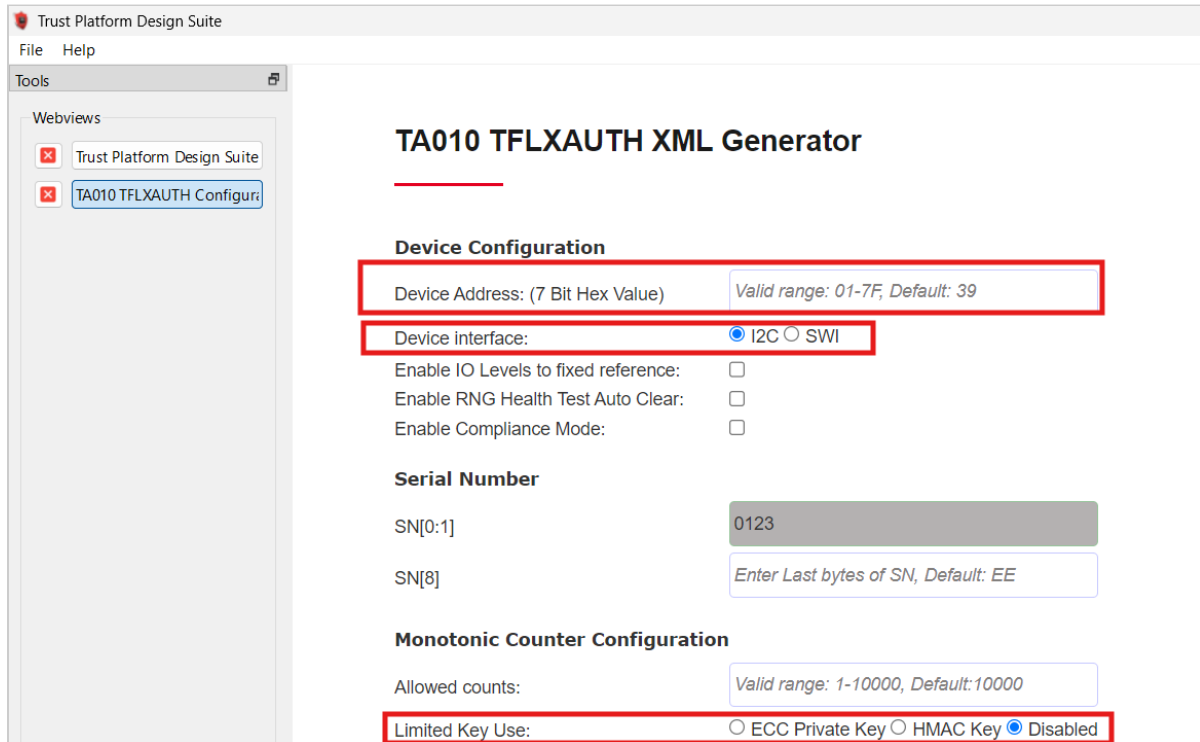


Figure-9

Proto Provisioning

- After adjusting configuration, scroll down and click on **Provision Prototype Samples**.

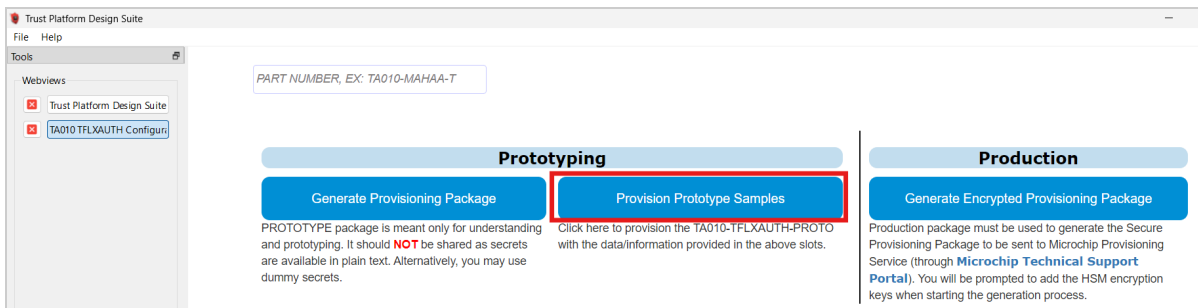


Figure-10

- Wait for the provisioning process to complete. The following result is observe:

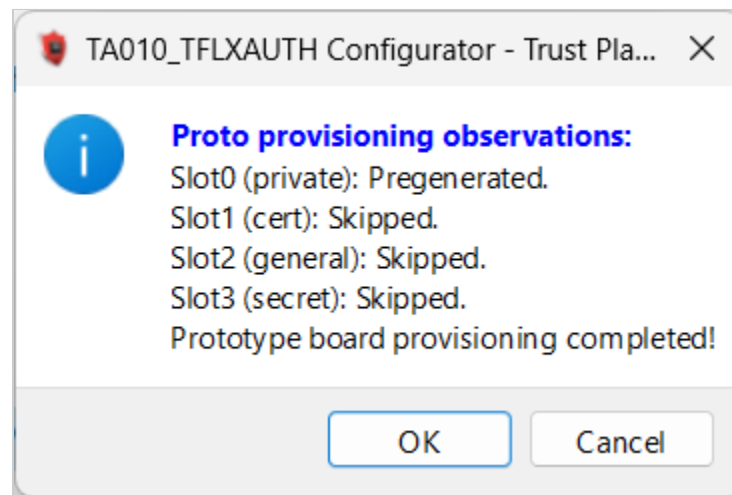


Figure-11

- Click on **OK** to close the success dialog.
- After provisioning, power cycle the device by disconnecting and reconnecting the USB cable.

Provisioning Usecase Resources

This step provisions the device for the specified use case. It gathers the necessary resources, generates the firmware resources, and provisions the device accordingly.

- Double-check that you selected the right target development kit.

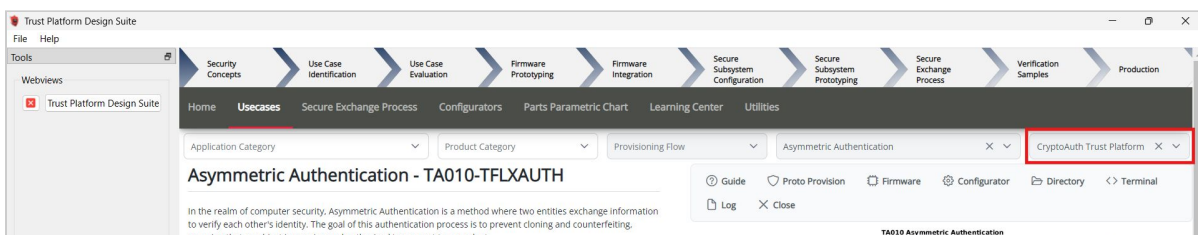


Figure-12

- Click on Proto Provision

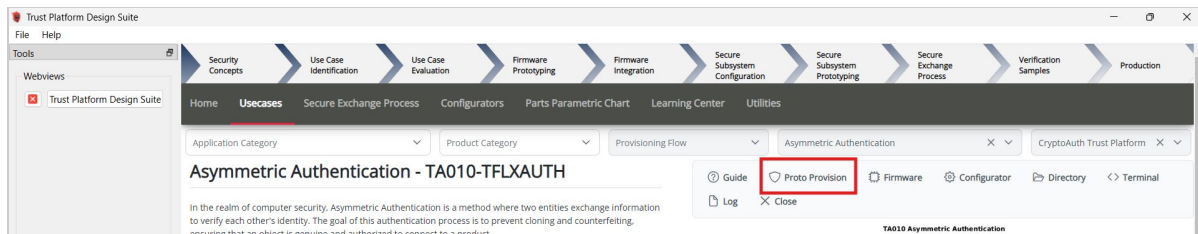


Figure-13

- Select the User Options:
 - Choose the Device Interface, the same interface selected in the configurator.
 - To Generate Certificates:
 - Select the **Generate** option within the **Certificates** section.
 - Enter the Organization Name for generating certificates in the **Organization Name** text box.
 - Enter the Validity in years for the Root Certificate in the **Root Certificate** text box.
 - Enter the Validity in years for the Signer Certificate in the **Signer Certificate** text box.
 - Enter the Validity in years for the Device Certificates in the **Device Certificate** text box.
 - Validity can range from 0 to 127 years; entering 0 will set the certificate expiration date to the year 9999, indicating it will not expire.
 - Choose the Generate option to create new private keys or upload user-specific keys for the Root and Signer private keys.

 The image shows the 'User Inputs' dialog box. It has a title bar with a maximize icon and a close icon. The main content area is divided into several sections. The 'Device Interface' section has two radio buttons: 'I2C' (selected) and 'SWI'. The 'Certificates' section has two radio buttons: 'Generate' (selected) and 'Upload'. Below these are four text input fields: 'Organization Name' (containing 'Microchip'), 'Root certificate' (containing '28'), 'Signer certificate' (containing '28'), and 'Device certificate' (containing '28'). Below these fields are two sections for private keys. The 'Root Private Key' section has a checked 'Generate' checkbox and a '+ Upload key' button. The 'Signer Private Key' section also has a checked 'Generate' checkbox and a '+ Upload key' button. At the bottom left is a 'reset' button, and at the bottom right is a 'Proto Provision' button.

Figure-14

- To Upload and reuse certificates:
 - Select the **Upload** option within the **Certificates** section.

- Upload the Root Certificate in the **Root Certificate** field.
- Upload the Signer Certificate in the **Signer Certificate** field.
- Upload the Signer Private Key in the **Device Certificate** field.
 - The Device Certificate will be tailored to the specific device, using the device serial number and public key for generation.
 - The Signer Private Key is necessary for generating and signing the Device Certificate.
- The **Root Private Key** and **Signer Private Key** fields are unused in this case.

Figure-15

- Click on Proto Provision
- The necessary resources will be created in the usecase working directory `~/trustplatform/symm_auth_ta010`:
 - **project_config.h** : Includes the selected interface for communication with the TA010 device.
 - **cust_def_device.c**: Contains the Generated Device Certificates Template and compressed certificate definition in C. A dummy public key will generated and used during resource generation. While Provisioning Device, Public key will be replaced by reading the device public key.
 - **cust_def_signer.c**: Contains the Generated Signer Certificates Template and compressed certificate definition in C.
 - **Root_cert.pem**: Contains Generated/Uploaded Root certificate in PEM format.
 - **Signer_cert.pem**: Contains Generated/Uploaded Signer certificate in PEM format.
 - **Device_cert.pem**: Contains Generated Device certificate in PEM format.
 - **Root_key.pem**: Contains Generated/Uploaded Root Private Key.
 - **Signer_key.pem**: Contains Generated/Uploaded Signer Private Key.
 - **Device_pub_key_SN.pem**: Contains Device Public Key Read from device.

- To open the use case working directory containing the use case resources Click on the **Directory** button .

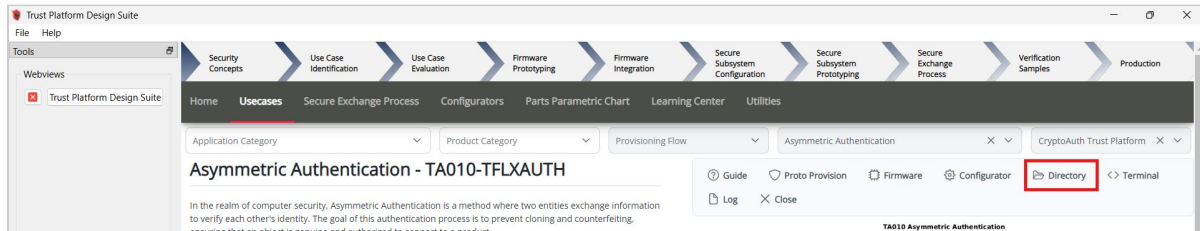


Figure-16

- Click Yes in the pop-up to load resources into TA010. A confirmation pop-up will appear once the loading process is complete.

Build and Program Application

- Make sure the MPLABX path is set in File -> Preferences -> MPLABX path.

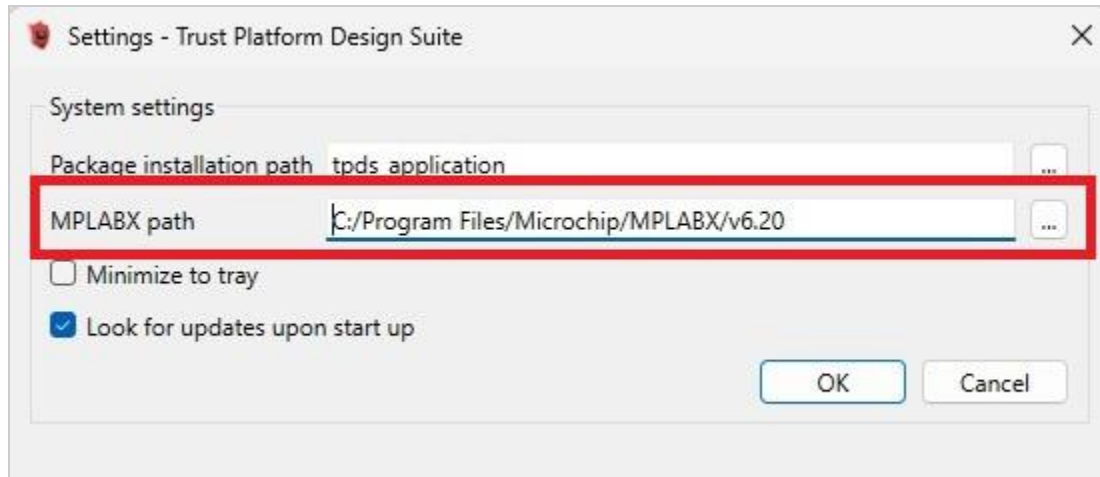


Figure-17

- Once the resources have been successfully loaded, open the Firmware Project by clicking on the Firmware button.

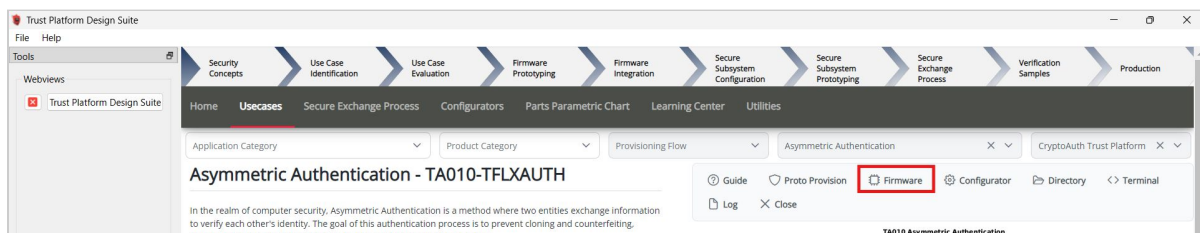


Figure-18

- The project **asymm_auth_ta010** will open in the MPLABX IDE.
- Right-click on **asymm_auth_ta010** and select "Set as Main Project".

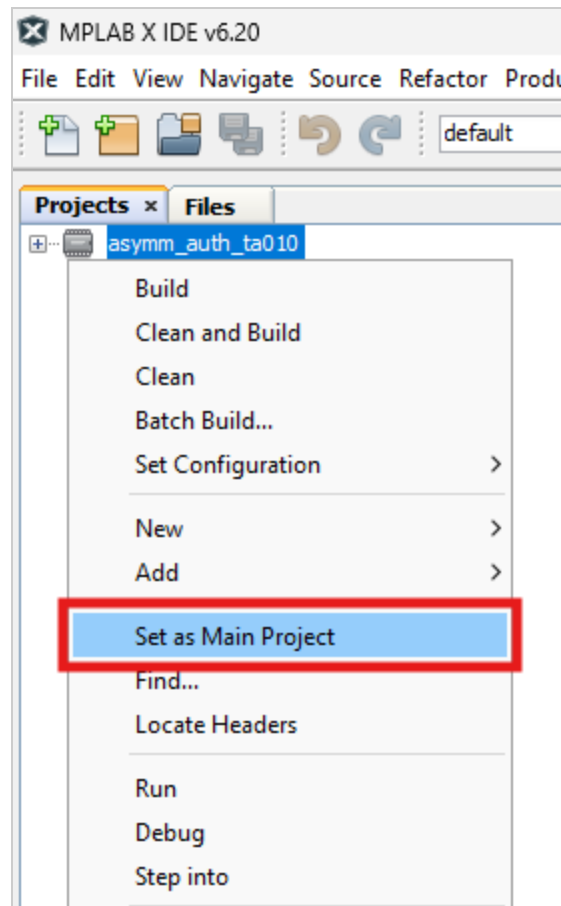


Figure-19

- Click on "Make and Program Device".

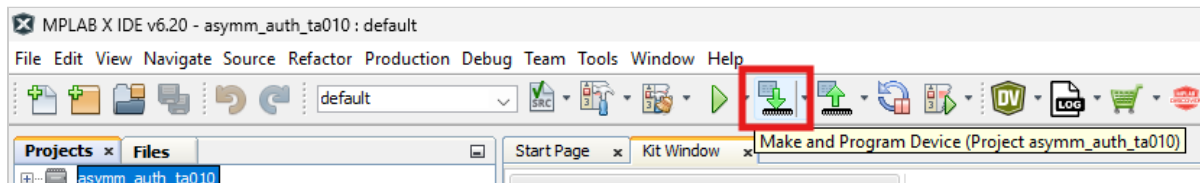


Figure-20

- Once the programming process is complete, please launch the Terminal application (e.g., Tera Term) on your computer if it has not been set up initially.
 - Connect to the Virtual COM port and configure the serial settings as follows:
 - Baud : 115200
 - Data : 8 Bits
 - Parity : None
 - Stop : 1 Bit
 - Flow Control : None
- Press the Reset button on Cryptoauth Trust Platform Development Kit
- The console will display a message indicating that the asymmetric authentication was successful.

- Review the output message in the console:

```

DEVICE: Rebuilt Signer Certificate:
-----BEGIN CERTIFICATE-----
MIIBvzCCAWSgAwIBAgIQfUT00eNo0mf5AqLSQ6lyJTAKBggqhkJOPQQDAjAqMQ0w
CwYDVQQKDARNQ0hQMRkwFwYDVQQDDBBNaWYb2NoaXAgUm9vdENBMCAxDTI1MDQw
NDA4MDAwMFoYDzIwMzUwNDA0MDgwMDAwWjAuMQ0wCwYDVQQKDARNQ0hQMR0wGwYD
VQQDDBRNaWYb2NoaXAgU2lnbmVyRkZGRjBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABPhzIPCiJaZJSovX3b6lCy5JuGxkyqDXPiqPJL8ILZRUzX68KDZK5UZOQDDM
P8fIvJVWrv3mYtARgn64aHubcsKjZjBkMA4GA1UdDwEB/wQEAwIBhjASBgNVHRMB
Af8ECDAGAQH/AgEAMBOGA1UdDgQWBBQlrFOEGuGGi8DhOMkDRdShrF0u0zAfBgNV
HSMEGDAWGBT7baxnlOFjRDxmd7z2l8qRyp05JjAKBggqhkJOPQQDAgNJADBGAiEA
hhZjFmDm3e/WdGppRJtbI3IRQwP5bkGfrWNF9g74zIQCIQDMLGkzmEitIX5qV6y2
TNuyBRJgm6lj67oZwIcEB606RQ==
-----END CERTIFICATE-----

DEVICE: Rebuilt Device Certificate:
-----BEGIN CERTIFICATE-----
MIIBuzCCA WKgAwIBAgIQfAcfFsqeXtF5br/iUKm8hzAKBggqhkJOPQQDAjAuMQ0w
CwYDVQQKDARNQ0hQMR0wGwYDVQQDDBRNaWYb2NoaXAgU2lnbmVyRkZGRjAgFw0y
NTA0MDQwODAwMDBaGA8yMDM1MDQwNDA4MDAwMFowLjENMAsGA1UECgwETUNIUEd
MBsGA1UEAwUc24wMTIzRTRBNzFCNDlFrkQ4RUUwWTATBgcqhkJOPQIBBggqhkJOP
PQMBBwNCAAR0lFQMrVJ2f/cAMQFdS+8E6NNXCASm9prz/zmeubcwqThKDvgnTy2h
xZLdGmXGh2v15mDtwB/37kKXeS33xvMco2AwXjAMBgNVHRMBAf8EAjAAMB0GA1Ud
DgQWBBTluUoJxqQK0Sm0AddCt4ZgXhdLFjAfBgNVHSMEGDAWGBQlrFOEGuGGi8Dh
OMkDRdShrF0u0zA0BgNVHQ8BAf8EBAMCA4gwCgYIKoZIj0EAwIDRwAwRAIg0ZSU
iHYGHPENnS3Yg7JUwlb4x0EYBT3C7Rtx+6FFewsCIHRil05ncjai061svvTR3TXZ
qgreEPeQ5KJocyUC984f
-----END CERTIFICATE-----

HOST: Signer certificate verified against root public key!
HOST: Device certificate verified against signer public key!

HOST: Generated challenge:
94 12 FB 0F A7 9A 52 E8 11 4F F4 83 78 A6 DB 36
62 A6 A6 BD 1C 1B FA 1B E3 55 D6 81 73 CA D8 B4

DEVICE: Calculated response for host challenge:
1E 23 10 24 8B 59 CC 0B BC B3 FF 58 0B C3 CE 13
AC DD 28 54 F5 21 70 46 7B 23 79 BD 59 F7 99 07
7D 0D 3F A3 C5 75 79 7B 10 24 1C 88 68 86 43 5D
51 CC 93 83 63 0A EF 18 22 68 DF 38 4A 8D 57 3D

HOST: Device public key from certificate:
74 94 54 0C AD 52 76 7F F7 00 31 01 5D 4B EF 04
E8 D3 57 08 04 A6 F6 9A F3 FF 39 9E B9 B7 30 A9
38 4A 0E F8 27 4F 2D A1 C5 92 DD 1A 65 C6 87 6B
F5 E6 60 ED 58 1F F7 EE 42 97 79 2D F7 C6 F3 1C

HOST: Device response to challenge verified!

Accessory device authenticated successfully

```

Figure-21

Conclusion

The outlined use case demonstrates the configuration of the TA010-TFLXAUTH device for asymmetric authentication, utilizing ECC and ECDSA algorithms to ensure secure accessory or disposable authentication. This comprehensive guide covers the setup of the Cryptoauth Trust Platform Development Kit, the provisioning of a blank TA010 device, and the generation of necessary cryptographic resources. It concludes with the steps to build and program the firmware, ultimately verifying the successful implementation of asymmetric authentication through the TA010-TFLXAUTH secure element.

Microchip Information

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **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 (FAQs), technical support requests, online discussion groups, Microchip design partner 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

Product Change Notification Service

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

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

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

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.

- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications 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. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. 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 ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

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, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge,

ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, TimeCesium, TimeHub, TimePictra, TimeProvider, and ZL 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, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mSiC, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICKit, PICtail, Power MOS IV, Power MOS 7, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, Turing, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, 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.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks 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.
 © 2024, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.
 ISBN: 978-1-6683-0382-5

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.