

TA010 Symmetric Authentication

TPDS Usecase Guide

Table of Contents

TA010 Symmetric Authentication	3
Description	3
Training Video	3
TA010 Symmetric Authentication	4
Prerequisites	4
Setting up Cryptoauth Trust Platform Development Kit (DM320118)	4
Setting up for Usecase.....	5
Opening the TA010 Symmetric Authentication Usecase	6
Provisioning Blank TA010 Device	7
Open TA010-TFLXAUTH Configurator.....	7
Provisioning Usecase Resources	9
Build and Program Application	11
Conclusion	13
Microchip Information	14
The Microchip Website	14
Product Change Notification Service	14
Customer Support.....	14
Microchip Devices Code Protection Feature	14
Legal Notice	15
Trademarks	15
Quality Management System.....	16

TA010 Symmetric Authentication

This application example demonstrates symmetric authentication using the Microchip TA010-TFLXAUTH device for accessory/disposable authentication with a diversified symmetric key authentication method.

Description

- The master symmetric key is securely stored in the Host Secure Element, while a derived key (derived from a root symmetric key and the Secure Element serial number) is stored in the Accessory Secure Element.
- Storing the master symmetric key in the ATECC608 ensures that the master key remains protected and is never exposed.
- In this example application, the Host Secure Element is the ATECC608, and the Accessory Secure Element is the TA010.

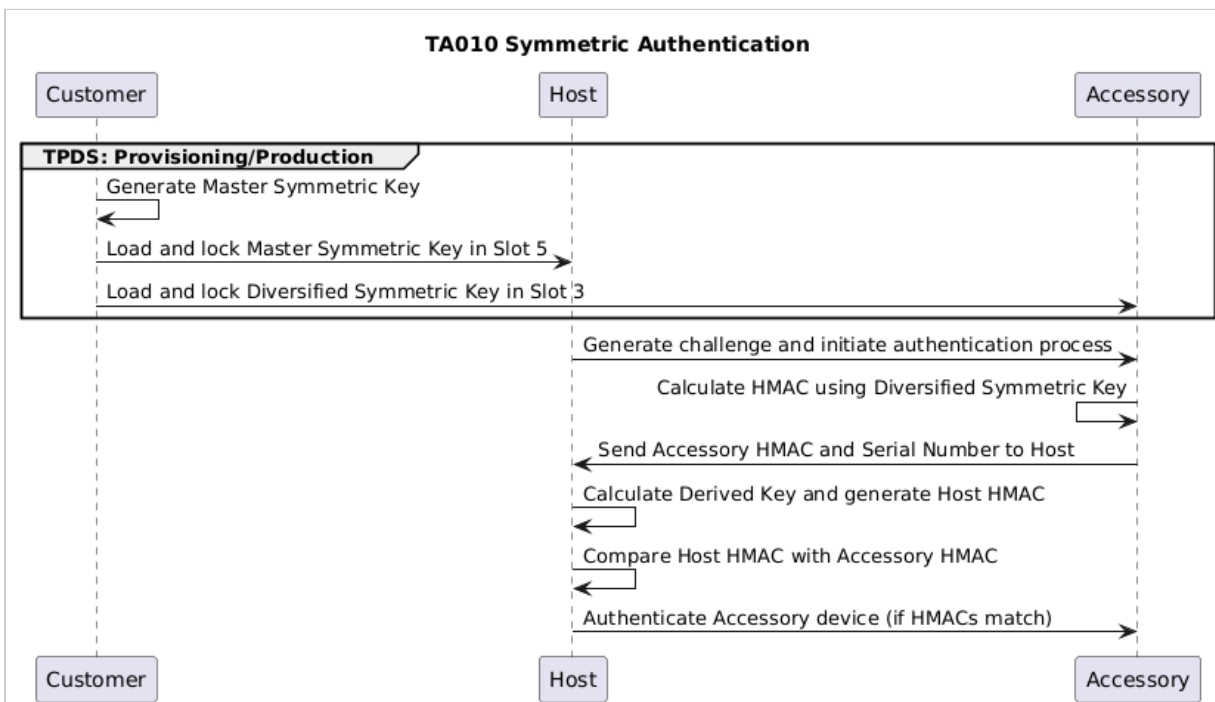


Figure-1

Training Video



Figure-2

TA010 Symmetric 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.

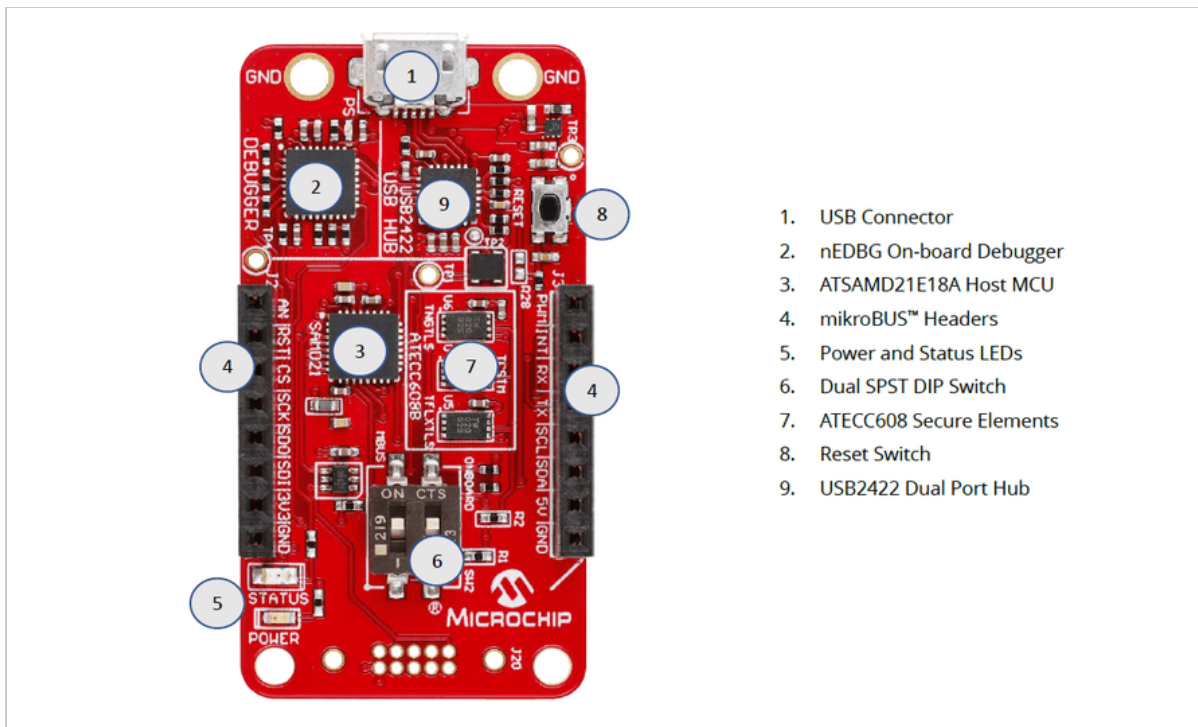


Figure-3

- 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 TA010 Socket board.

Setting up for Usecase

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

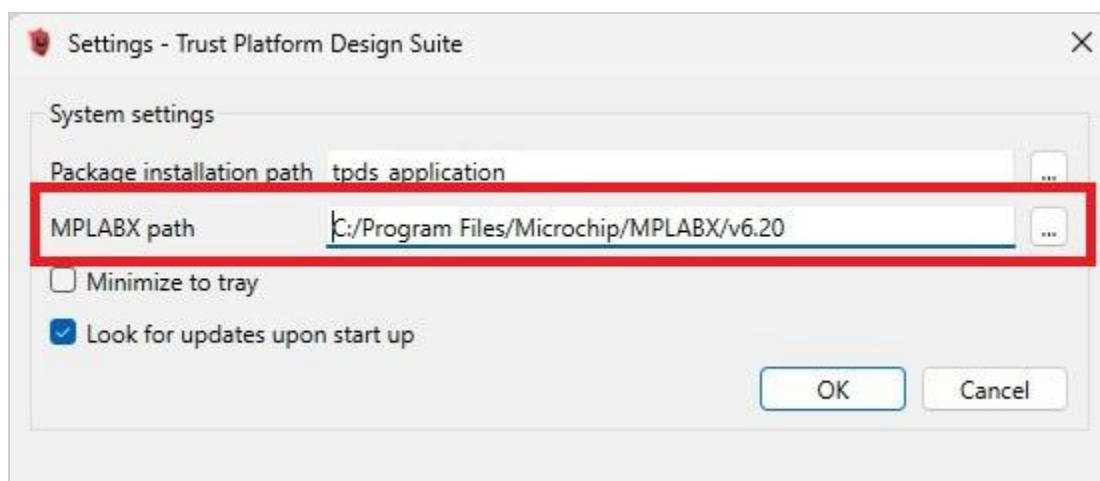


Figure-4

- 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 the following 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 Symmetric Authentication Usecase

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

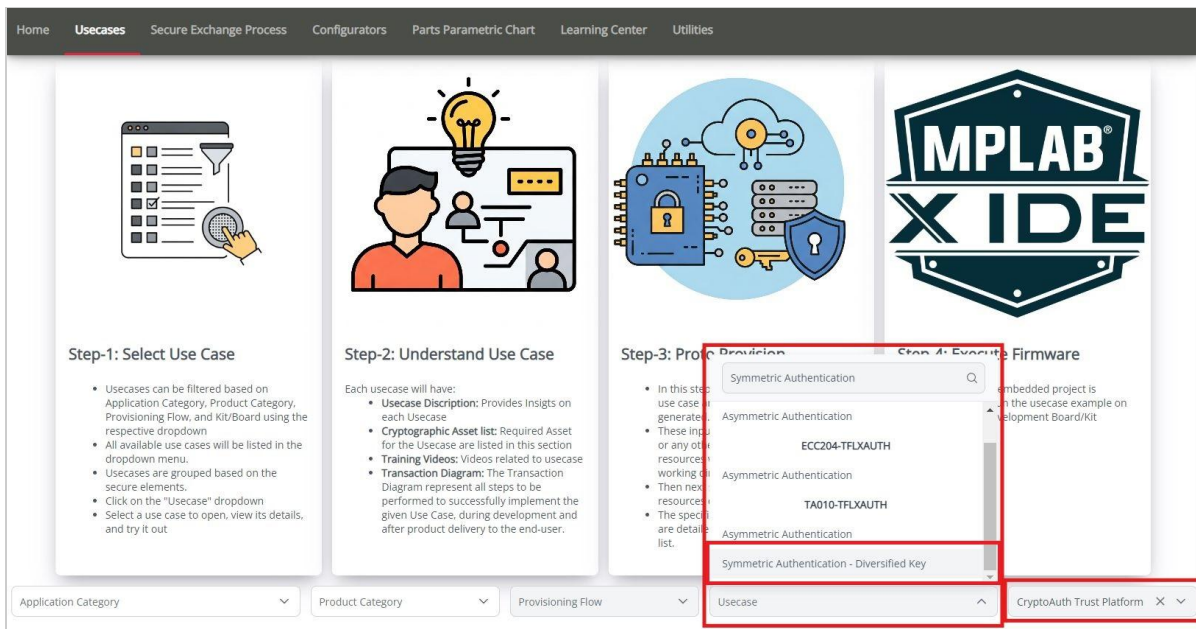


Figure-6

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

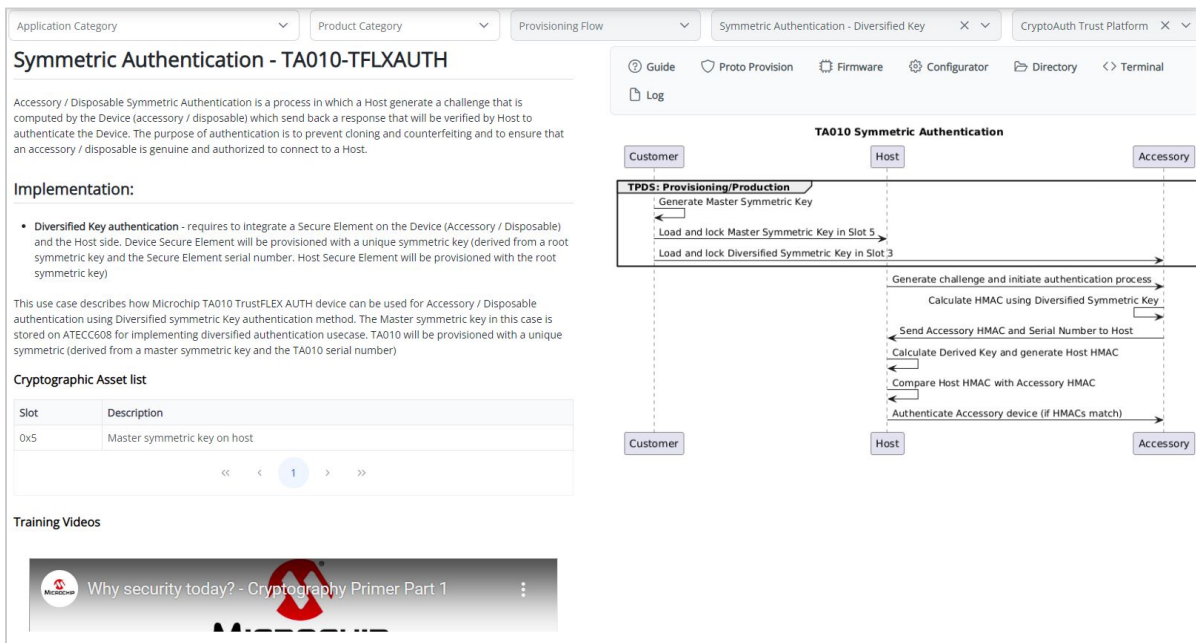


Figure-7

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.

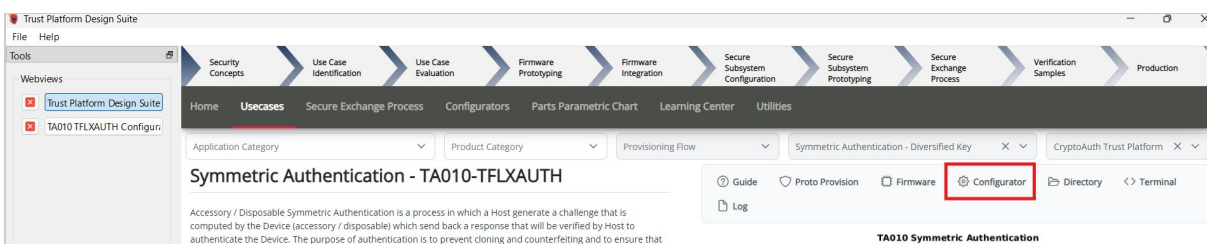


Figure-8

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.

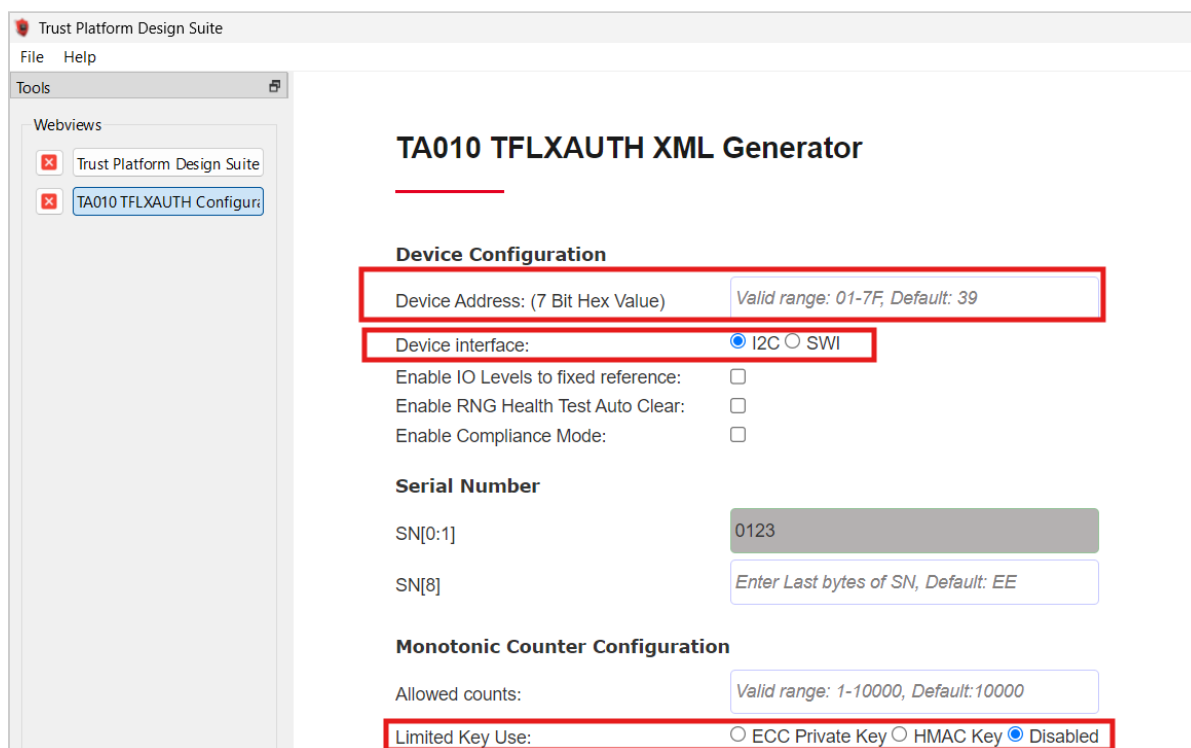


Figure-9

Proto Provisioning

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

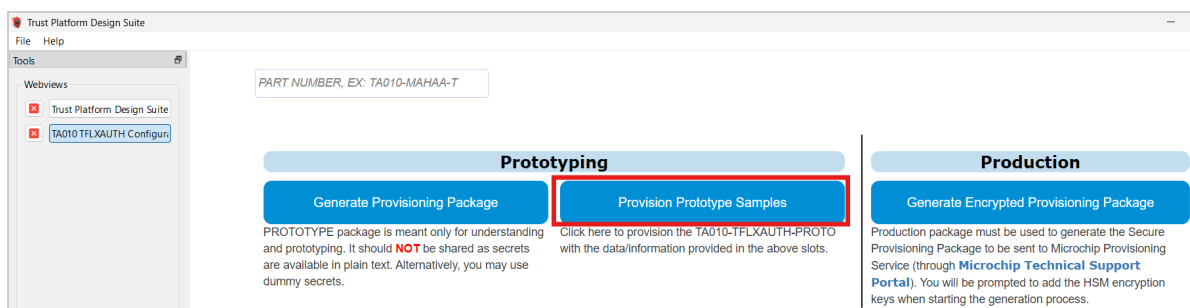


Figure-10

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

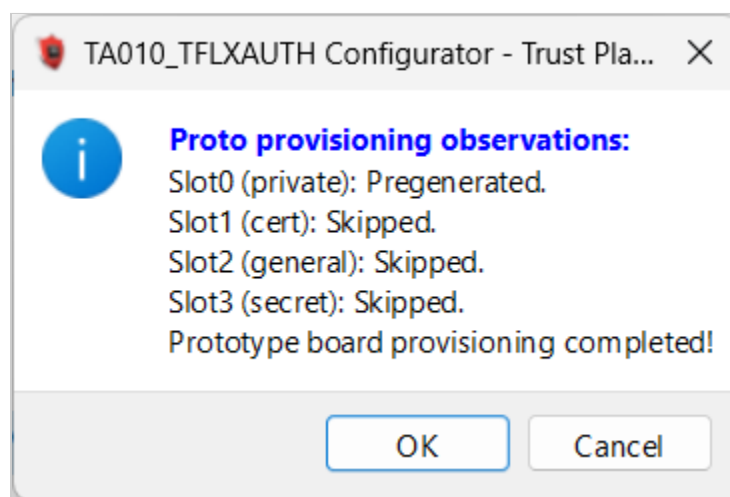


Figure-11

- 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.

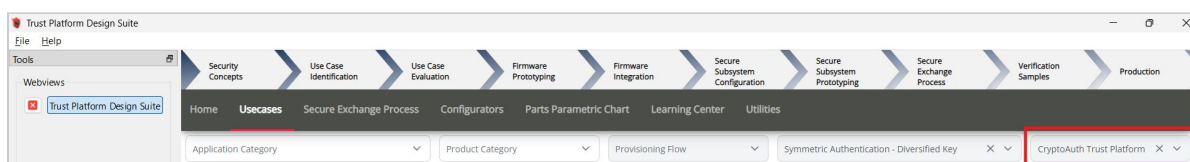


Figure-12

- Click on Proto Provision

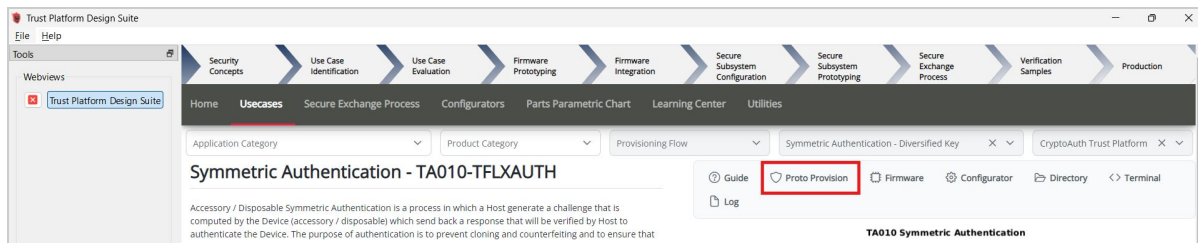


Figure-13

- Select the User Options:
 - Choose the Device Interface, the same interface selected in the configurator.
 - By default, the option to generate a new master symmetric key will be checked. If you prefer to use a user-specific symmetric key, use the upload option.
 - Click on Proto Provision

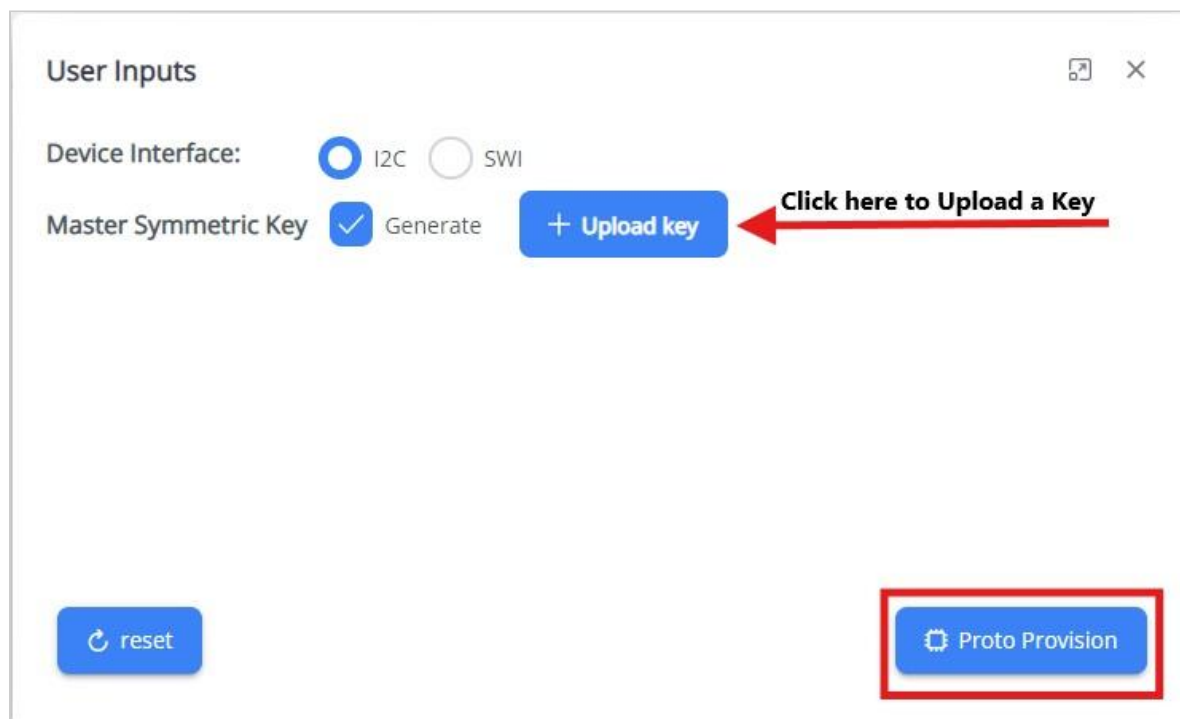


Figure-14

- 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.
 - **master_symm_key.pem** : Contains the generated/uploaded master symmetric key in PEM format.
- Click on the **Directory** button to open the use case working directory containing the use case resources.

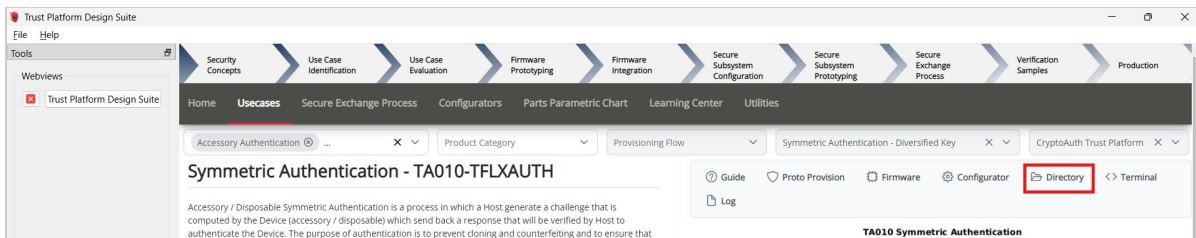


Figure-15

- Click Yes in the pop-up to load resources into the ATECC608 and 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.

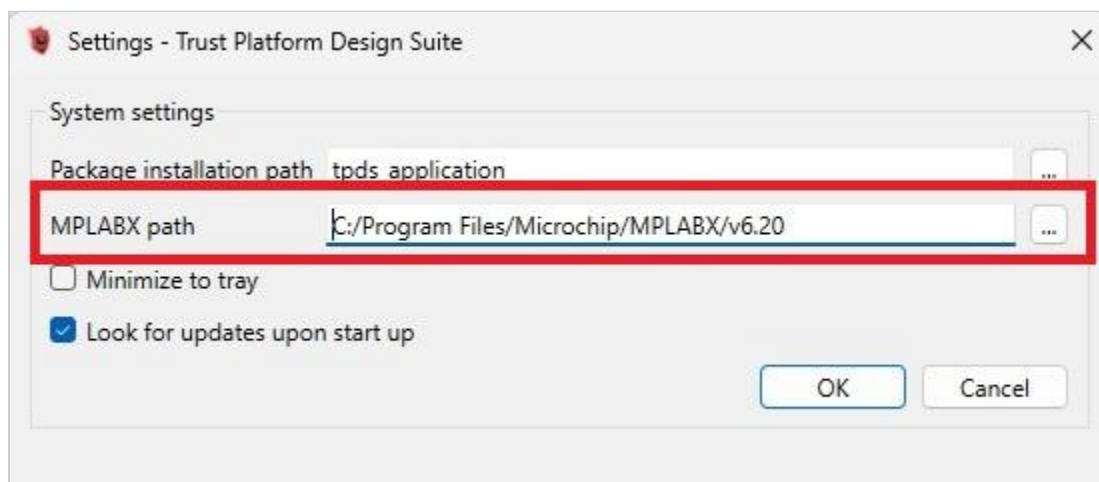


Figure-16

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

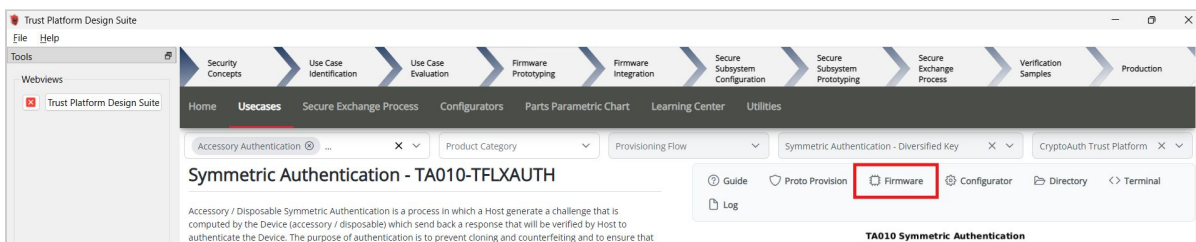


Figure-17

- The project **symm_auth_ta010** will open in the MPLABX IDE.
- Right-click on **symm_auth_ta010** and select "Set as Main Project".

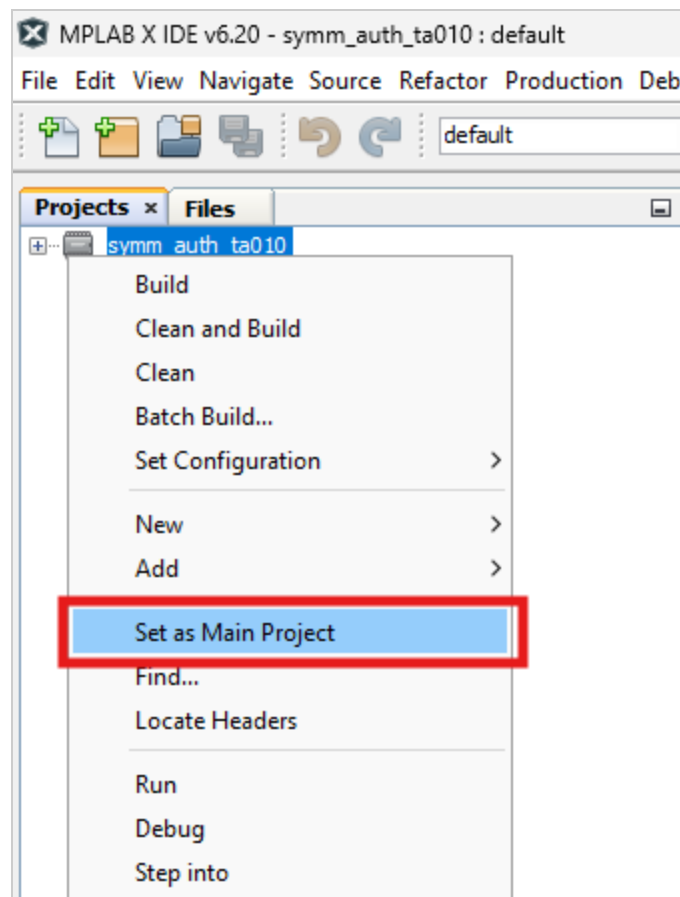


Figure-18

- Click on "Make and Program Device".

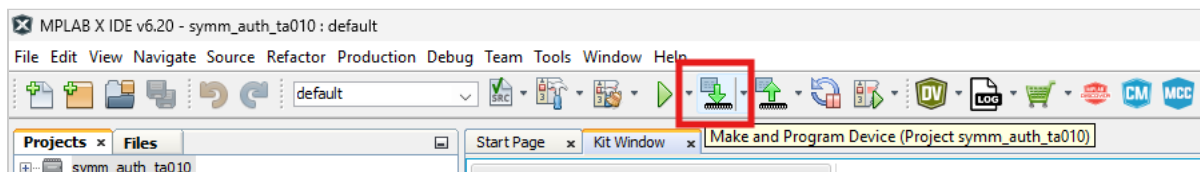


Figure-19

- 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 symmetric authentication was successful.
- Review the output message in the console:

```
Generated Host challenge:
F3 33 27 7A 27 ED A2 F9 7C 91 90 EF D8 5F EA 0E
F5 2E 63 E3 B5 1E 05 8C CB 5D C8 C9 B9 3A AE 04

TA010 Monotonic counter read status: 00 , Value:0

HMAC received from Accessory device:
62 C7 96 CD F7 3F 58 4A 7E 1D 1E 2A 29 88 2F 74
51 6A 1D 17 9F 66 BE 03 59 98 7E 0E C2 F7 03 12

TA010 Monotonic counter read status: 00 , Value:0

HMAC calculated on the Host:
62 C7 96 CD F7 3F 58 4A 7E 1D 1E 2A 29 88 2F 74
51 6A 1D 17 9F 66 BE 03 59 98 7E 0E C2 F7 03 12

Accessory device is authenticated successfully.
```

Figure-20

Conclusion

The outlined usecase demonstrates the configuration of the TA010 as a client accessory, with an ATECC608 as a host, to securely implement a Derived Symmetric Key system. This concludes the overview, transaction diagram, proto provisioning, and firmware steps associated with Symmetric Authentication using the TA010 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.