

TA010 WPC Authentication

TPDS Usecase Guide

Table of Contents

TA010 WPC Authentication	3
Description	3
Training Video	4
TA010 WPC Authentication	5
Prerequisites	5
Setting up Cryptoauth Trust Platform Development Kit (DM320118)	5
Setting up for Usecase.....	5
Opening the TA010 WPC Authentication Usecase.....	7
Provisioning Blank TA010 Device	8
Open TA010-TFLXWPC Configurator.....	8
Provisioning Usecase Resources	9
Build and Program Application	11
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 WPC Authentication

The purpose of this Use Case is to authenticate a Qi 1.3 Wireless Power Charger from a mobile phone, as Qi 1.3 specification mandate the usage of a Secure subsystem (Secure Element) on the charger side. It is based on a standard asymmetric authentication

Asymmetric Authentication is a process based on a custom PKI (Public Key Infrastructure) where a Host (mobile phone) will authenticate that the WPC charger (device) is genuine. The Host will first verify the Signer certificate (Manufacturer) device certificates (Product Unit Certificate PUC) based on the Root CA Public key and will generate a challenge to be signed by the charger private key. The Host will then perform an ECDSA verify command to ensure that the signed challenge is valid.

This use case describes how Microchip TA010-TFLXWPC Secure Subsystem can be used for Qi 1.3 WPC authentication using asymmetric authentication (Custom PKI based).

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 Manufacturer Certificate and verifies the certificate with the Authority Public key(Root).
 - Upon successful verification, the Host requests the Product Unit Certificate and verifies it using the Manufacturer Certificate.
 - The Host requests WPC Chain Digest and verifies the WPC Chain Digest.
- **Challenge-Response:**
 - The Host generates a random number challenge and sends it to the TA010-TFLXWPC.
 - The TA010-TFLXWPC 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.

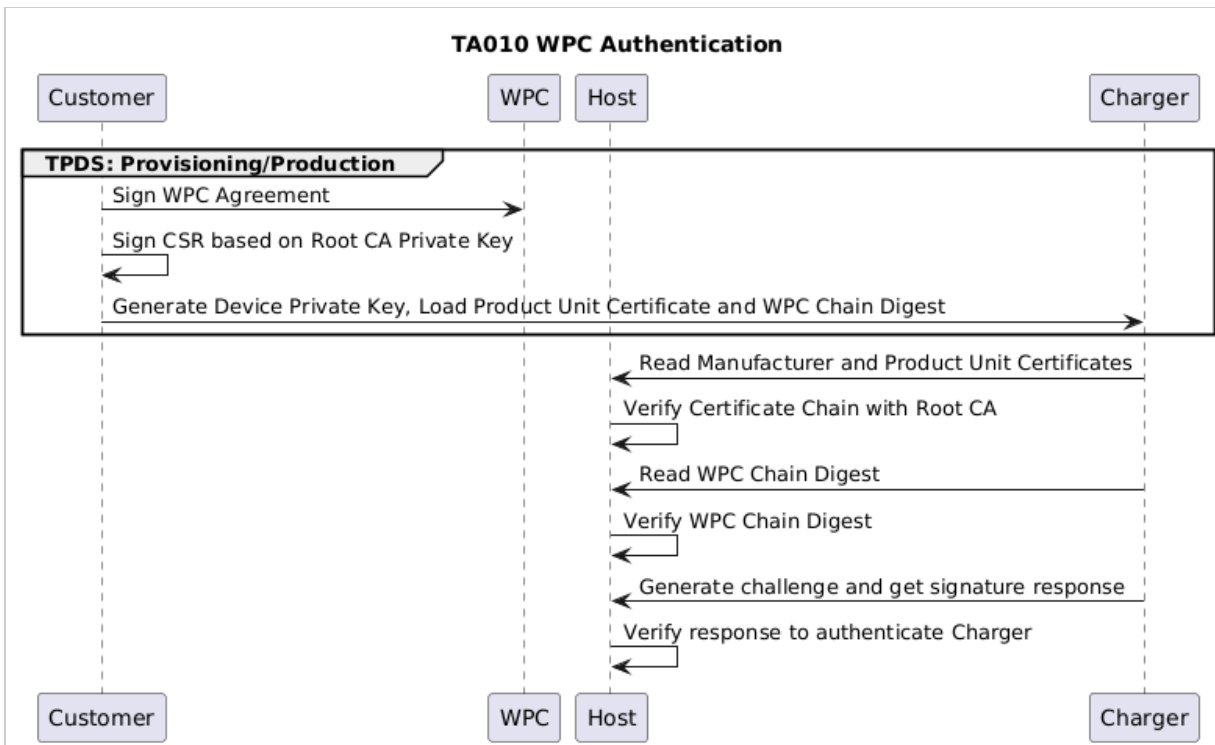


Figure-1

Training Video



Figure-2

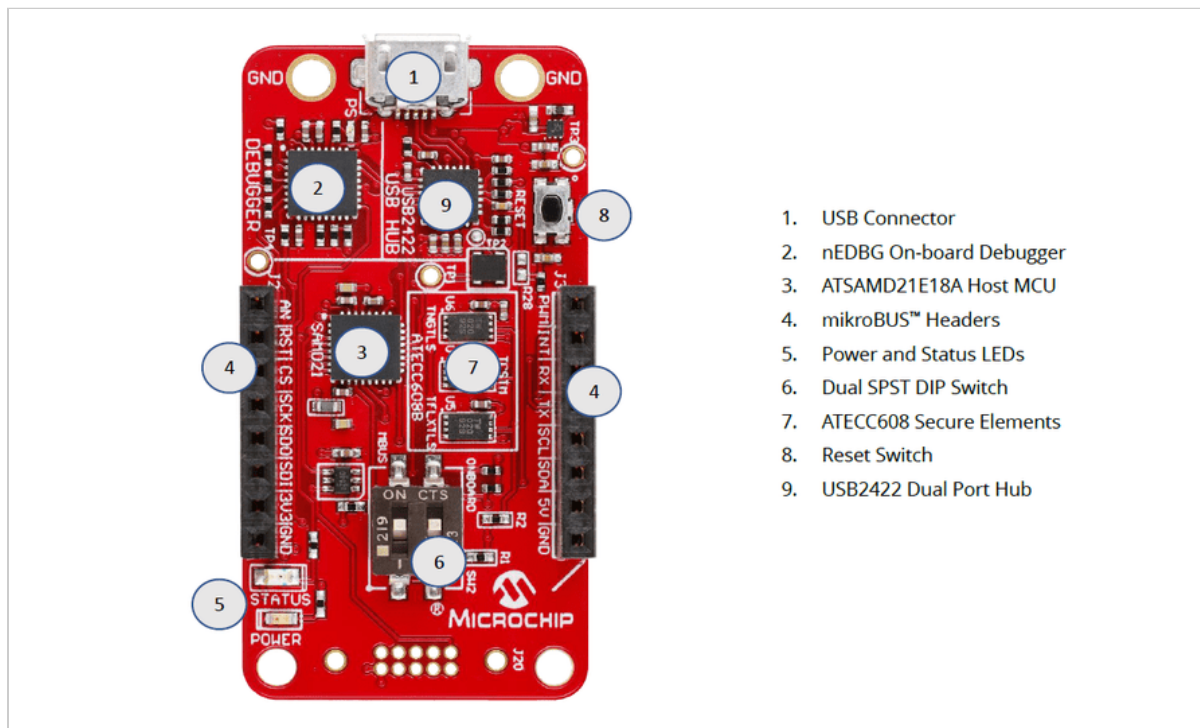
TA010 WPC Authentication

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.



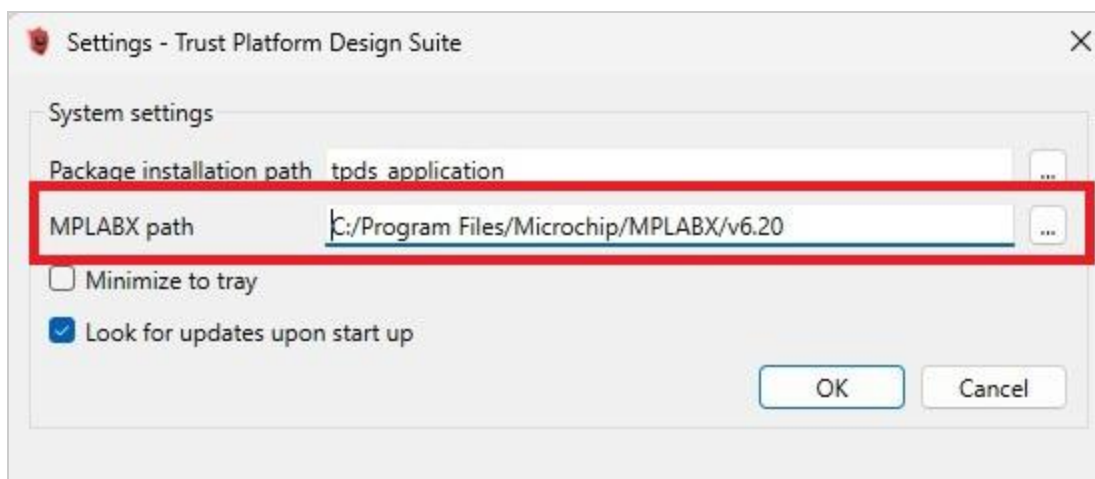


Figure-4

- 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 WPC Authentication Usecase

- Open TPDS and navigate to Usecases Section.
- Select the kit as **CryptoAuth Trust Platform**.
- Select Application Category as **WPC**.

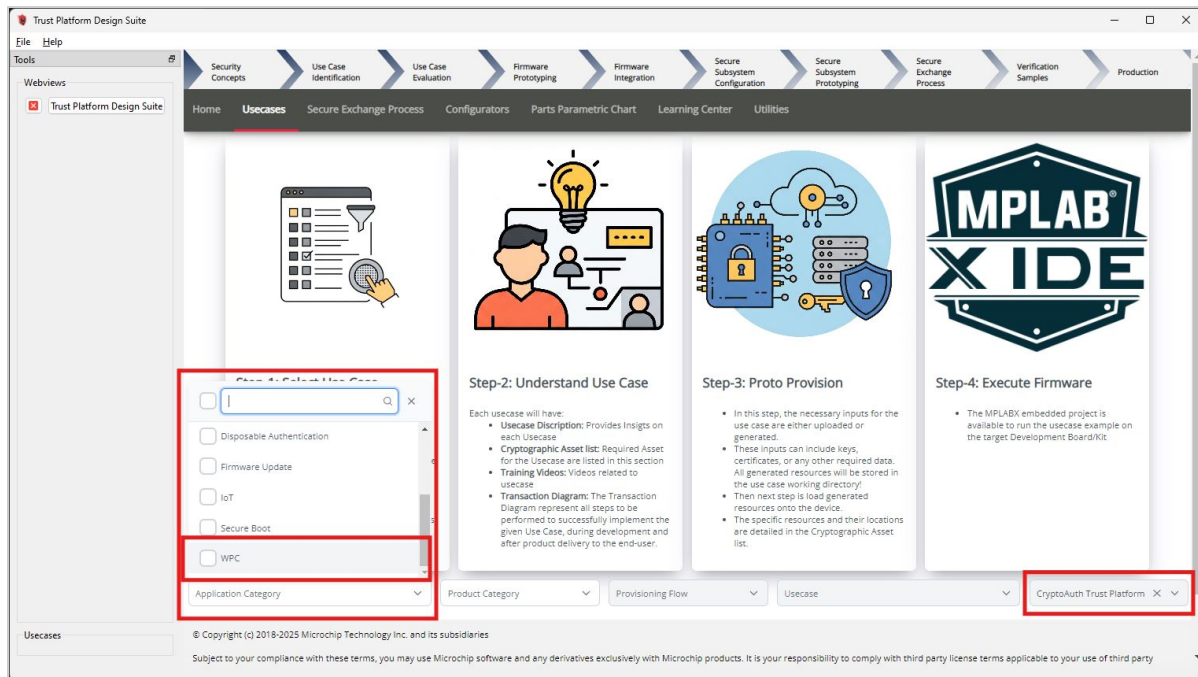


Figure-6

- Select Usecase as **WPC Authentication** under TA010-TFLXWPC.

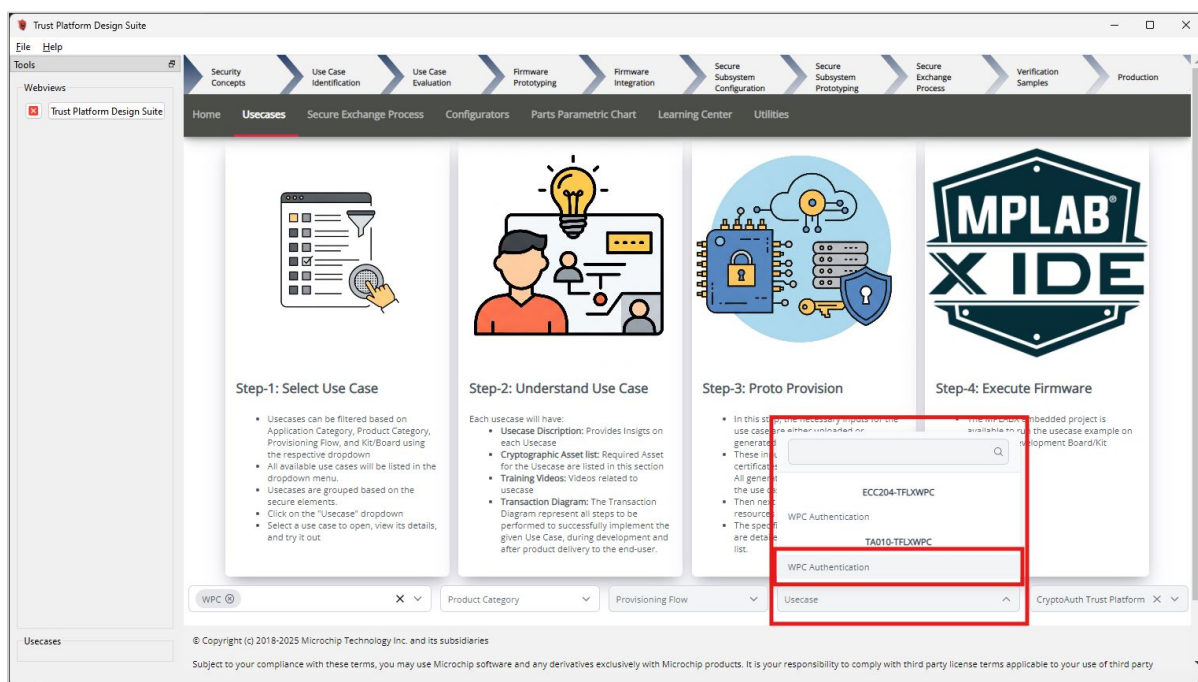


Figure-7

- The TA010-TFLXWPC - WPC Authentication usecase will open as below:

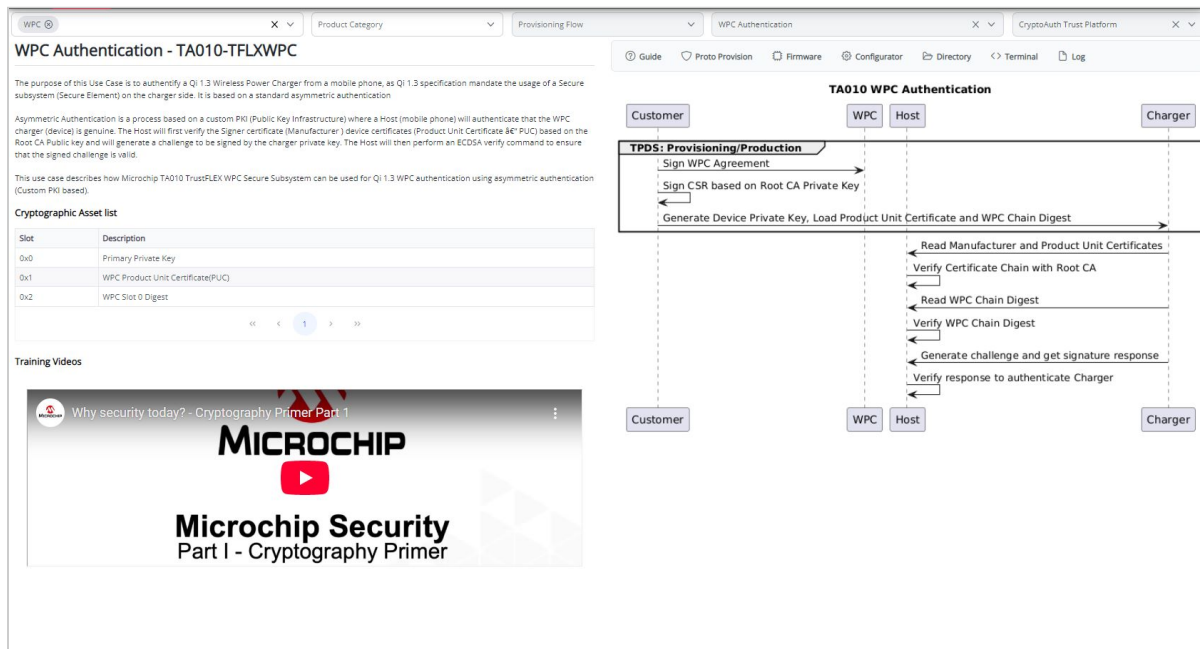


Figure-8

Provisioning Blank TA010 Device

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

Open TA010-TFLXWPC Configurator

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

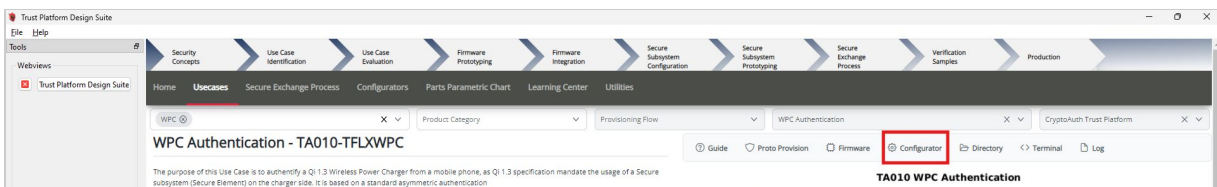


Figure-9

Adjust the Configuration

Once the TA010-TFLXWPC Configurator is open:

- Leave the Device address empty to configure with the default TFLXWPC address. **The use case requires the device to be configured with the default TFLXWPC address.**

Proto Provisioning

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

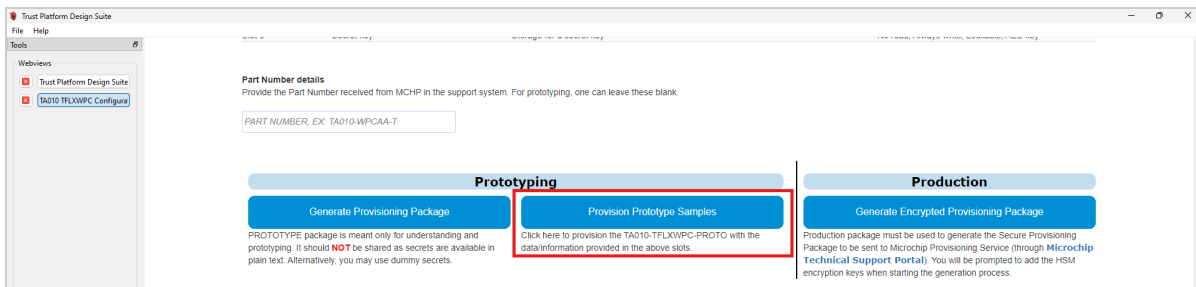


Figure-10

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

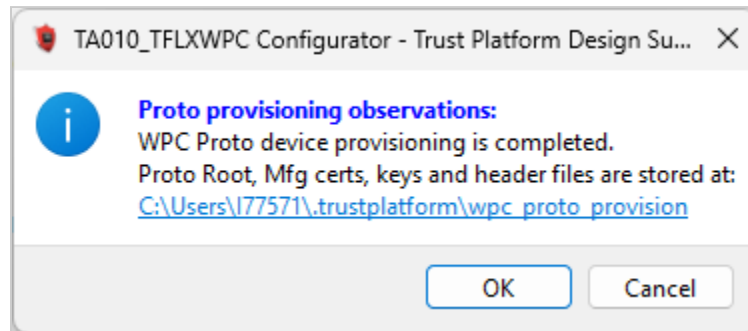


Figure-11

- 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.

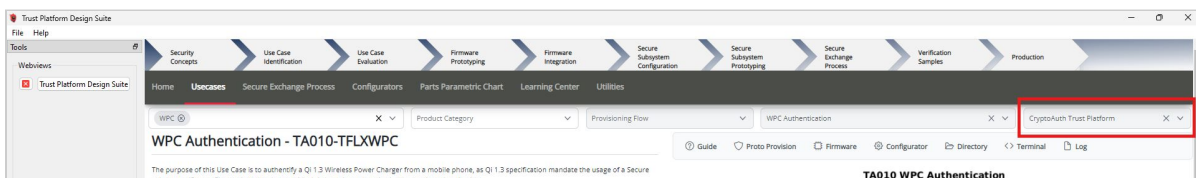


Figure-12

- Click on Proto Provision

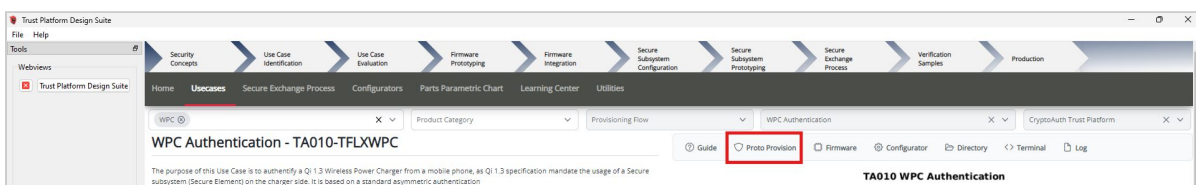


Figure-13

- Provide the User Inputs:
 - Enter **PTMC Code**, **Qi ID** and **CA Sequence ID** in respective input fields. For prototyping, these fields can be left blank, and default values will be used.
 - Choose the Generate option to create new private keys or upload user-specific keys for the Root and Manufacturer private keys.
 - Click on Proto Provision

The screenshot shows a web interface titled "User Inputs". It contains three input fields: "PTMC Code" (with a default value of 0x004E), "Qi ID", and "CA Sequence ID". Below these are two sections for key management: "Root Key" and "Manufacturer Key". Each section has a "Generate" checkbox and an "Upload key" button. The "Manufacturer Key" checkbox is checked. A "reset" button is located at the bottom left, and a "Proto Provision" button is at the bottom right. Red rectangular boxes highlight the key management section and the "Proto Provision" button.

Figure-14

- The necessary resources will be created in the usecase working directory `~/trustplatform/wpc_auth_ta010`:
 - **ta010_tflxwpc.h**: This file contains generated Root, Manufacturer certificates and other data in c, which is useful for firmware project.
 - **wpc_root_cert.crt**: This file contains generated Root Certificate.
 - **wpc_mfg_{PTMC CODE}-{CA Sequence ID}.crt**: This file contains generated Manufacturer Certificate.
 - **wpc_puc_ta010_{SN}.crt**: This file contains generated PUC Certificate.
 - **wpc_root_key.pem**: This file contains generated/uploaded Root Private Key.
 - **wpc_mfg_{PTMC CODE}-{CA Sequence ID}_key.pem**: This file contains generated/uploaded Manufacturer Private Key.
 - **device_pub_key_{SN}.pem**: This file contains Product Unit Public Key Read from device.
- To open the use case working directory containing the use case resources Click on the **Directory** button .

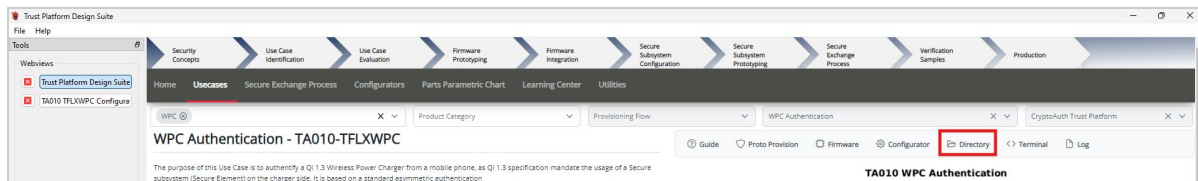


Figure-15

- 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.

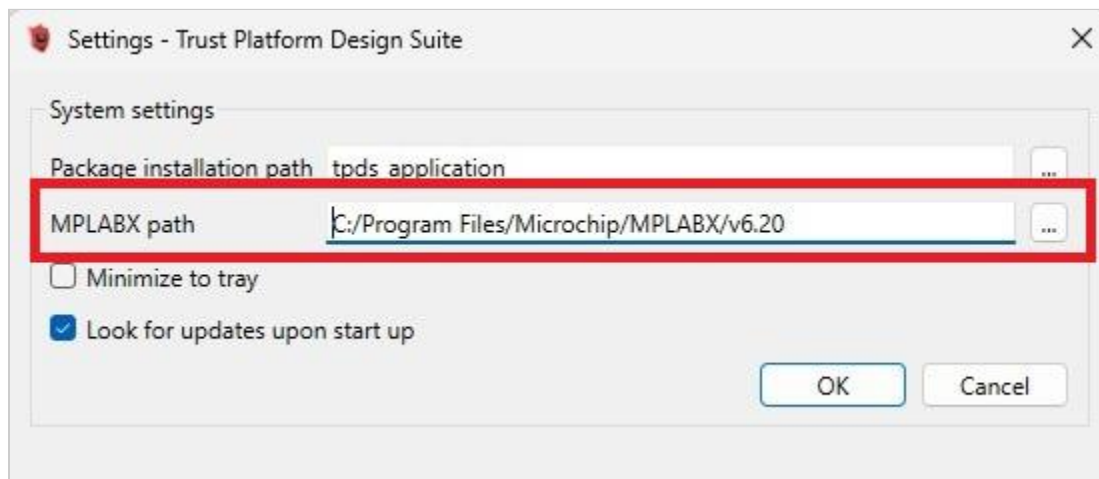


Figure-16

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

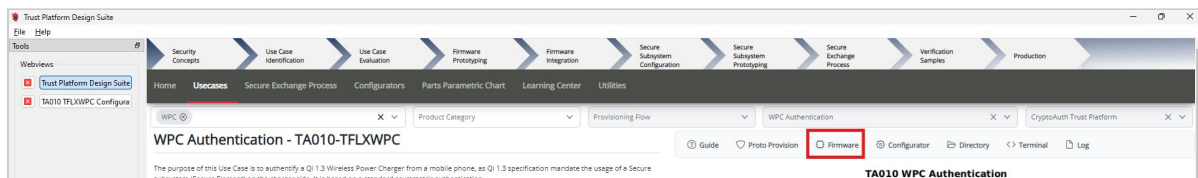


Figure-17

- The project **wpc_auth_ta010** will open in the MPLABX IDE.
- Right-click on **wpc_auth_ta010** and select "Set as Main Project".

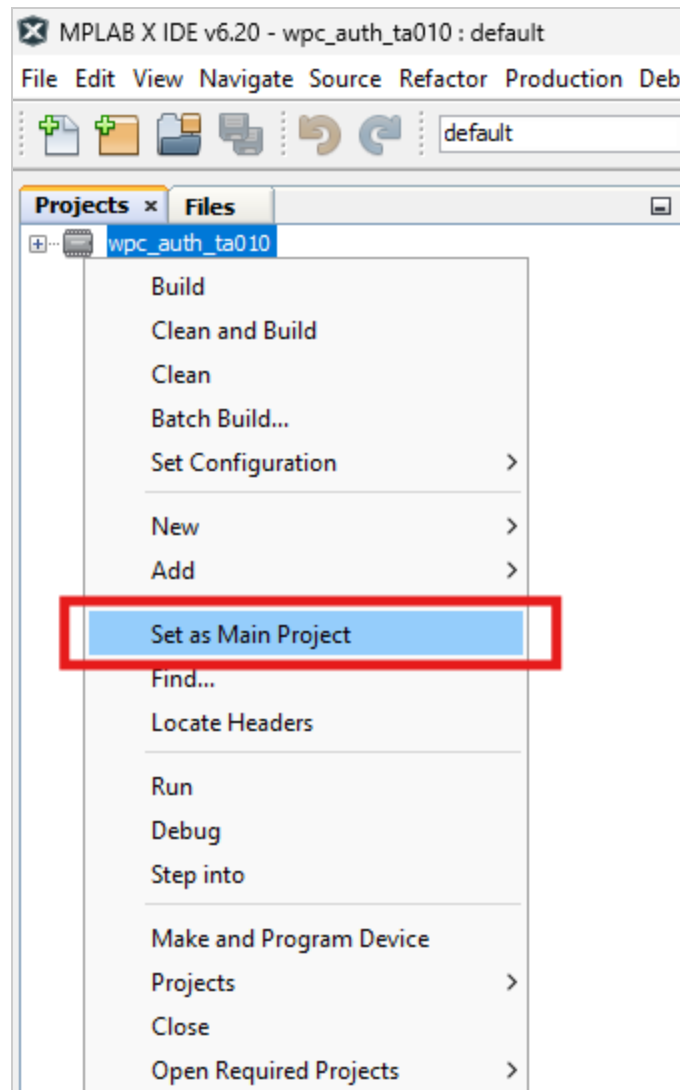


Figure-18

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

```

WPC Product Unit Certificate (PUC):
30 82 01 38 30 81 DE A0 03 02 01 02 02 08 7C A4
AB 1E 1A 8D 77 3A 30 0A 06 08 2A 86 48 CE 3D 04
03 02 30 12 31 10 30 0E 06 03 55 04 03 0C 07 30
30 34 45 2D 30 31 30 22 18 0F 32 30 32 35 30 35
30 35 30 34 30 30 30 30 5A 18 0F 39 39 39 39 31
32 33 31 32 33 35 39 35 39 5A 30 11 31 0F 30 0D
06 03 55 04 03 0C 06 30 31 31 34 33 30 30 59 30
13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE
3D 03 01 07 03 42 00 04 75 BE 07 7A 12 A4 94 BD
23 46 E5 2E E1 43 16 45 5B 09 99 B3 2C EF E7 16
35 A1 24 9E C3 C7 F3 A9 31 D7 A2 A4 DF 76 2F E4
DD 18 DD FD 38 33 9A DF DF F8 D7 CF 23 C4 F1 E3
D6 0F E2 4D D4 82 9E CA A3 1B 30 19 30 17 06 05
67 81 14 01 02 01 01 FF 04 0B 04 09 00 00 00 00
00 8B D7 61 2F 30 0A 06 08 2A 86 48 CE 3D 04 03
02 03 49 00 30 46 02 21 00 A7 97 42 11 AC 96 D6
FE 6E 44 69 F2 62 4C 88 8B 79 8A 82 50 23 2B 5A
7D 31 64 8E 80 DA 60 98 28 02 21 00 CE 2D 2D 00
05 60 87 C2 15 47 0E 83 CF 45 E4 57 DA CE 48 7F
3F D2 1F 34 D9 8D 32 E1 93 DF D4 13

Verify Root Certificate against its public key... OK
Verify Mfg Certificate against root's public key... OK
Verify PU Certificate against root's public key... OK

Certificate Chain (Host calculated digest):
82 1C 78 BA 75 48 D8 EE F2 4A 4D 9D 47 9E 4B 64
76 3B 2B 2A DE 9B FF C9 36 4C A3 0E 09 FA 3B F9

Certificate Chain (Device digest):
82 1C 78 BA 75 48 D8 EE F2 4A 4D 9D 47 9E 4B 64
76 3B 2B 2A DE 9B FF C9 36 4C A3 0E 09 FA 3B F9

Comparing host and device chain digest values... OK

Power Receiver: Generated challenge:
74 01 81 5A 58 1D 1E 22 8D BA 6F 7F D5 AA 86 D6
8F EF 3B 9E B7 C0 32 7F 71 3B 92 A5 2E 48 E6 BF

Power Transmitter: Challenge response:
13 AA 4A 22 6F 6A 7C E5 3E 5D 7C 50 70 92 D8 27
7E 41 10 81 2A B7 D0 48 BF 80 78 AB 35 D6 02 C9
9C 8D F7 BC D4 01 0B 84 BF 43 4B 56 98 1B 44 46
C9 B7 29 57 52 2A 3A AA EB 71 40 36 CD AF 5A A5

Power Receiver: Verify response: OK

Power Receiver - Transmitter challenge response is verified!

WPC Chain and Chain digest based authentication is successful!

```

Figure-20

Conclusion

The outlined use case demonstrates the configuration of the TA010-TFLXWPC device for WPC authentication, utilizing ECC and ECDSA algorithms to ensure Secure subsystem (Secure Element) on the charger side. 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 WPC authentication through the TA010-TFLXWPC 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.